

XINGNET NGS-3324TG 交换机

用户配置手册

(第-版, 2004-2-12)

广东网域科技有限公司

网址：www.xingnet.cn

support@vavic.com

目录

第一部分 硬件安装指导

使用说明

内容索引

该部分主要针对如何安装 NGS-3324TG 交换机进行了论述。主要包括该交换机的特性，交换机的构成组件，以及各个组件所完成的功能。具体内容列示如下：

- ✧ 第 1 章 NGS-3324TG 交换机综述　　论述了交换机的特性，各项性能指标，各个面板的说明以及模块说明。
- ✧ 第 2 章　安装方法　　讨论了 NGS-3324TG 交换机的环境要求，如何安装交换机、如何将串口连接到交换机以及首次登录的一些信息。

使用者知识要求

在阅读本部分时，要求读者具备一定网络知识。这要求读者最好熟悉以下知识：

- 局域网（Local Area Network）（LAN）
- 以太网概念（Ethernet Concept）
- 以太网交换和桥概念（Ethernet Switching and Bridging Concepts）

术语解释

主干	作为网段间传输通信量的主要路径的网络
带宽	网络信道的频带宽度,通常表示网络信道传输数据的能力
10BASE—T	IEEE 802.3 简略术语,表示在 3 类或更好的双绞线电缆上基于曼彻斯特信号编码的 10Mbps 以太网
100BASE--TX	IEEE 802.3 简略术语,表示基于 4B/5B 信号编码和使用两对 5 类双绞线电缆的 100Mbps 快速以太网
100BASE--FX	IEEE 802.3 简略术语,表示在光纤上基于 4B/5B 信号编码的 100Mbps 快速以太网
自动协商	自动协商模式是端口根据另一端设备的连接速率和双工模式,自动把它的速率调节到最高的公共水平,即线路两端能具有的最快速率和双工模式
全双工	一种允许设备同时接收和发送数据的通信方法
半双工	一种通信方法,设备在某一时刻只能发送或接收数据
广播风暴	由于以太网上大量的广播帧造成网络阻塞,引起网络故障
RJ--45	双绞线链路中使用的一种 8 针模块连接器
MDIX	交叉的介质有关接口,它将一台设备的发送信号送到另一台设备的接收信号端,反之亦然

第1章　NGS-3324TG 交换机综述

注意：在使用该交换机之前，请务必先认真阅读本使用手册，以避免因误操作而损坏交换机。

1.1 产品规格

NGS-3324TG 以太网交换机基于高性能的 ASIC，采用模块化的结构设计；提供 24 个 1000Base-FX(SFP)单/多模光接口以及 4 个 10/100/1000BASE—TX 复用以太网接口，支持基于端口的 802.1Q VLAN；具有端口捆绑/负载均衡，Spanning Tree，端口镜像，IGMP Snooping 等特性。NGS-3324TG 是一款性能卓越的核心汇聚交换机，是目前极具竞争力的园区网及企业网中的核心汇聚以太网交换机解决方案。

1.2 功能特点

强劲的交换处理能力：

- 无阻塞交换结构，功能强劲的专用 ASIC 进行包转发处理，所有端口可同时工作在线速状态。
- 大容量共享包缓存区，先进的包头阻塞（HOL）预防机制，最大限度地减小包阻塞提供优化的转发性能。

1.3 性能指标

表 1-1 性能指标

特性		NGS-3324TG
端口配置	基本配置	24 个 1000Base-FX(SFP)单/多模光接口以及 4 个 10/100/1000BASE—TX 复用以太网接口
	扩展插槽	
上行连接		
容错设计		CPU 寻检
端口汇聚		6 组，每组可汇聚 8 个端口
协商功能		10/100/1000Mbps 自适应
基本性能		
MAC 地址		16K
缓存大小		32MB
转发模式		Store-and-forward.
网络和流量控制		
流控		IEEE802.3X；背压式
VLAN		802.1Q
Spanning Tree		支持
优先级		IEEE802.1p
管理特性		

SNMP	V1、V2c、V3
RMON	1、2、3、9
HTTP	支持
CLI	支持
支持标准	IEEE 802.1d; IEEE 802.1p; IEEE 802.1Q;IEEE802.3ad; IEEE 802.3; IEEE802.3u; IEEE 802.3X; IEEE802.3z;
SNMP/RMON	MIB (RFC1213); Ethernet==LIKE MIB(RFC1643); Bridge MIB(RFC1493); RMON MIB(RFC1757); RIP V2 MIB(RFC1724);
状态指示	端口：LINK,ACT 通用：电源状态、系统状态，AUX 的 LINK,ACT
最大线缆长度	10/100/1000BASE—T: 3、4、5 类屏蔽/非屏蔽双绞线 100 米; 100BASE—FX: 62.5/125um 多模光纤(最大 2km)、9um 单模光纤(最大 15km) ;
电气特性	
安规	IEC 950,EN60950(CE),UL 1950/CSA22.2—950; AS/NZ 3260
电磁兼容性	FCC Part 15, Subpart J, Class A; EN55022(CISPR:1993), Class A; VCCI Class A ITE; C—tick; IEC 1000-4-2; IEC 1000-4-3; IEC 1000-4-4; IEC 1000-4-5;
接口类型	10/100/1000BASE-TX：RJ--45 100BASE—FX：SFP 控制台管理接口：RJ--45
物理尺寸（长×宽×高）	440 ㎜×280 ㎜×44.5 ㎜
重量	5.5 kg
工作环境	
温度	0~50℃
湿度	10~90%无凝结
电源	180—260VAC ，47—63Hz 或 44—53VDC

功耗	30W

1.4 整机组成

1.4.1 前面板组成部分

前面板由以下几部分组成：

- 1 个 CONSOLE 串口，1 个 AUX 口
- 24 个 1000BASE—FX 光接口
- 4 个 10/100/1000BASE—TX 自适应以太网复用端口
- 1 个 POWER 状态指示灯
- 1 个 SYSTEM 状态指示灯 STATUS
- 1 个 AUX 口的 LINK 指示灯
- 1 个 AUX 口的 ACTIVE 指示灯
- 24 个 LINK 状态指示灯
- 24 个 ACTIVE 状态指示灯

1.4.2 前面板各个部分功能

提供 1 个 RJ45 型的 RS—232C 控制口(concole)，以便通过其对 NGS-3324TG 交换机进行带外管理。

提供 1 个 AUX 口，可对 NGS-3324TG 交换机进行 WEB 页访问，配置以及管理，软件升级等。缺省状态下，AUX 口的 IP 地址为：192.168.1.168/24。

4 个 10/100/1000Mbps 以太网复用接口，支持 5 类 UTP/STP 网线，可与 PC、服务器、其他 HUB 或交换机直接相连。

前面板上提供有网口工作状态及系统工作状态两组易于理解的 LED 指示灯，便于诊断网络上所发生的各种问题和故障。各指示灯的详细定义如下：

表 1—2 NGS-3324TG 指示灯详细定义

LED		状态		说明
系统状态指示	POWER	绿色	点亮	在交换机加电约 0.5 秒钟之后，此指示灯应该长亮
			暗	没有加电或电源系统工作不正常
	STATUS	绿色	闪烁	当交换机在加电自检后，系统工作正常时指示灯会闪烁
			暗或常亮	系统工作不正常
1000M 网络端口状态	LINK	绿色	长亮	当端口与所连接的设备建立了稳定的连接之后，该端口所对应的指示灯长亮。
			暗	没有连线或该网口连接不正常
	ACT	双色	闪烁	该网口正在进行数据收发

指示			暗	该网口没有数据发送

1.4.3 后面板组成部分

- 1 个电源开关和 1 个电源插座，用于连接 180-260V（50-60Hz）的交流电源。

1.4.5 侧板

在 NGS-3324TG 交换机的右侧是几排散热通风孔，左侧有两个系统散热风扇， 用于进行降温散热，改善系统的温度特性，保证交换机的工作正常。特别要注意的是不要堵住通风孔，而且在交换机的两侧必须要有足够的空间，方便空气流通，使得散热正常。否则，会导致无法散热，影响机器正常工作，有可能会导致机器损坏。

第2章　安装方法

2.1 装箱清单

- 1 台 NGS-3324TG 交换机
- 1 套机架安装配件（两个支架和数个螺丝）
- 1 根电源线
- 1 根 UTP5 直连网线
- 1 个供配置的 RJ45 转 DB9 的转接头
- 1 只光盘（NGS-3324TG 交换机的说明书,包含硬件安装指导和软件配置指导）

以上清单，如有缺损，请立即与分销商或者与生产商的销售人员联系。建议保留好原包装盒，以便更换时使用。

2.2 安装方法

特别提示：为了不影响交换机正常工作，一定要确保交换机的两侧和后面保留至少 10 厘米的空间；同时，不能让交换机右侧的散热孔阻塞，以便交换机左侧的风扇很好的排气。

2.2.1 安装在桌面上

1. 从包装盒中找到四个橡皮脚
2. 揭去四个橡皮脚上的衬片
3. 将四个橡皮脚安装到交换机的下面（以确保交换机放置稳固），放置在固定的桌面上。
4. 当然，一定要确保入风口（左面）和风扇出口（后面的右部）没有被阻塞

2.2.2 安装到机架上

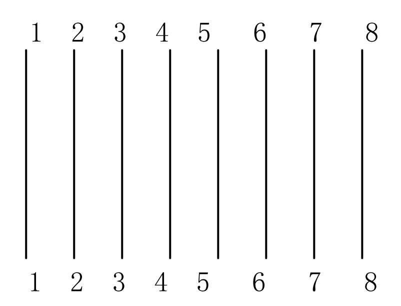
1. 交换机的包装盒中取出 8 个（每侧 4 个螺丝）黑色螺丝和两个机架片。
2. 将机架片的有 4 个螺丝孔的一边贴住交换机的左右两侧，注意交换机的两侧分别有 4 个螺丝孔与之相对应，然后分别将 4 个螺丝拧进去。
3. 机架片的另一侧是与机架配套用，将交换机移到机架上，找到要安装的位置，然后分别将机架片的 2 个大螺丝孔与机架上的大螺丝孔对应，并贴住，用螺丝拧上去即可，注意要拧紧，防止松动，从而使交换机能够稳固安装在机架上面。

2.3 连接交换机

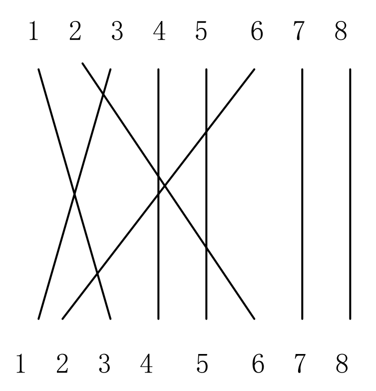
2.3.1 连接到以太网

千兆电口进行互联时，必须要用直通线（注意直通线的 8 个脚都要连起来）。下面是直通线，交叉线以及 console 口的 DB9 转 RJ45 的连接示意图，供用户参考。

网线制线



直通线示意图



交叉线示意图

CONSOLE 配置口电缆：RJ45 转 DB9

DTE

RJ45(插座)　　　　　　　　DB9（母插头）

1 RTS------------------------------8 CTS
2 DTR------------------------------6 DSR
3 TxD------------------------------2 RxD
5 GND------------------------------5 GND
6 RxD------------------------------3 TxD
7 DSR------------------------------4 DTR
8 CTS------------------------------7 RTS

说明：

RTS= Request To Send 请求发送端
DTR=Data Terminal Ready 数据终端就绪端
TxD= Transmit Data 发送数据端
GND= Ground 信号地端
RxD= Receive Data 接收数据端
DSR=Data Set Ready 数据线路设备就绪端
CTS=Clear To Send 允许发送端

2.3.2 连接配置口

NGS-3324TG 交换机提供了 RJ45 转 DB9 的转接头,可将转接头的 DB9 一端连 PC 的 RS232 串口,另一头通过直连网线连到交换机的 console 口，通过命令行来配置交换机，对交换同进行带外管理。连接到配置口用于系统管理员进行本地配置。

配置端口的设置如下所示：

波特率—9600

数据位—8

停止位—1

奇偶校验位—None

流量控制—无

连接到 console 端口的终端必须要有相同的配置。

2.3.3 连接电源

NGS-3324TG 交换机的电源为 220V 交流电源，在连接电源之前请仔细核实交换机电源规格，确保接入正确的电源相同，以免损坏交换机。

2.3.4 交换机加电

在完成交换机的安装，连接好交换机后，就可以给交换机加电了。当交换机正常加电后，交换机前面板上的 LED 状态指示灯将出现如下反应：

首先“Power”指示灯将点亮，“Status”指示灯开始闪烁，同时插有网线的端口的 ACT 指示灯将快速点亮，LINK 指示灯暗；然后交换机进行自检并开始加载系统软件，大约在 100 秒之后，其端口 “LINK”指示灯亮，表示交换机已进入正常工作状态, “ACT”开始闪烁,表示该端口进行数据收发。如果此时 Console 连接上了 PC，按步骤进入超级终端后，则在系统启动完成后屏幕上将出现 Login，具体配置方法参见本书的软件配置指导描述。

第二部分 软件配置指导

使用说明

内容索引

本文档对三层以太网交换机的配置方法做了详尽说明，对配置时所使用的命令或操作给予了详尽的解释。

本文档具体内容列示如下：

- 第 1 章 产品介绍　　简述产品的主要特性和功能列表。
- 第 2 章 管理交换机　　主要讲述系统的命令语法、用户权限的设置问题以及管理交换机的途径等。
- 第 3 章 配置交换机的端口　　对交换机端口的基本参数配置， 流控和广播抑制，端口带宽管理等内容做了详尽的阐述。
- 第 4 章 配置 VLAN　　主要讲述如何配置交换机虚拟局域网(VLAN),包括静态配置和动态 VLAN 注册协议的配置。
- 第 5 章 FDB 表　　主要讲述了 FDB 表的基本概念，以及一些基本参数的配置命令和查看 FDB 表的命令。
- 第 6 章 STP 协议　　讲述了生成树协议（Spanning Tree protocol）参数配置。
- 第 7 章 配置组播　　讲述配置几种组播的概念和配置，包括静态组播，GMRP 和 igmp snooping 协议。
- 第 8 章配置链路捆绑 Trunking　　主要讲述链路捆绑协议的简单原理和配置方法。
- 第 9 章配置访问控制列表（ACL）讲述了访问控制列表的特点，以及配置内容和方法。
- 第 10 章端口镜像(mirroring)　　主要描述端口镜象基本原理和配置方法。
- 第 11 章 Quality of Service(QoS)　讲述服务质量（QOS）控制规则，以及如何配置。
- 第 12 章配置虚拟接口　　详细阐述了配置交换机三层子接口的方法。
- 第 13 章配置路由　　描述配置交换机的静态路由，RIP 和 OSPF 协议的方法。
- 第 14 章 配置组播路由协议　　介绍了组播路由协议 PIM-SM 的配置方法。
- 第 15 章配置 802.1x　　详细介绍了 802.1x 的工作原理，以及如何进行配置。
- 第 16 章配置 Portal 认证　　详细描述了 portal 认证的工作原理及配置方法。
- 第 17 章配置 RADIUS　　详细描述了 RADIUS 协议的工作原理及配置方法。
- 第 18 章配置 DHCP Relay　　讲述了 DHCP 中继协议的配置方法。
- 第 19 章配置 DHCP SERVER　　讲述内嵌 DHCP 服务器的配置方法。
- 第 20 章 SNMP　　详细介绍了 SNMP 协议的工作原理，基本参数以及配置方法。
- 第 21 章 配置 ARP　　讲述了如何配置静态 IP 与 mac 地址映射表，以及如何查看地址映。
- 附录 常见故障诊断　　列举了交换机的一些常见故障以及出现故障的可能原因。

使用者知识要求

在阅读本手册时，要求读者具备一定网络知识,并有一定网络建设经验和网络设备配置经验。这要求读者最好熟悉以下知识：

- 局域网（Local Area Networks）（LANs）
- 以太网概念（Ethernet Concepts）
- 以太网交换和桥概念（Ethernet Switching and Bridging Concepts）
- 服务质量概念(Quality Of Service Concepts)
- 路由概念（Routing Concepts）
- 网络协议概念（Internet Protocol Concepts）
- 路由信息协议 RIP（Route Information Protocol Concepts）
- 开放式最短路优先协议 OSPF（Open Shortest Path Fist Concepts）
- Protocol Independent Multicast-Sparse Mode (PIM-DM) Protocol Specification
- IP 多播概念（IP Multicast Concepts）
- 因特网组播管理协议 IGMP（Internet Group Management Protocol）
- 简单网络管理协议概念 SNMP（Simple Network Management Protocol）
- 远程认证拨入用户服务 RADIUS （Remote Authentication Dial-In User Service）

注释符号说明

符　　号	含　　义
🚨	提示用户在使用过程中尤其要注意的地方。
☞	表示附加说明信息。

其他文档

交换机的其他文档主要包括：

- ♦ 硬件安装指导

第一章 产品介绍

本章针对产品的特性及其参数指标进行列示和说明，并对相关的技术给出简要解释。

1.1 产品描述

NGS-3324TG是一款24端口的全千兆三层以太网交换机。它既可以工作在网络的第二层，也可以工作在网络的第三层，并且实现二层数据和三层数据线速转发。

其接口配置如下

- 24 个1000Base-FX 光接口，4个10/100/1000BASE—TX复用端口
- 1 个控制口用于连接仿真终端进行交换机的配置管理(CONSOLE)
- 1个带外管理接口(AUX)

1.2 特性描述

支持IEEE 802.1Q和IEEE 802.1p标准的Virtual Local Area Networks (VLANs)
支持IEEE802. 1D标准的Spanning Tree Protocol（STP）
支持IEEE 802.3ad标准的端口捆绑（Trunk）
线速（Wire-speed）二层交换，三层路由转发
支持服务质量QoS（Quality of Service）
支持基于MAC地址、IP地址或协议端口号的绑定和访问控制（ACL）
支持端口镜像功能，可分输入、输出以及二层或三层镜像（Mirroring）
支持端口带宽管理（即带宽限制）
支持组播静态设置
支持IGMP snooping
支持VLAN注册协议(GVRP)
支持组播注册协议（GMRP）
支持针对VLAN级的DHCP (Dynamic Host Configuration Protocol) relay
支持内嵌的DHCP服务器
支持Routing Information Protocol (RIP) 版本1和版本2
支持OSPF（Open Shortest Path Fist ）开放式最短路径优先协议
支持Internet Group Management Protocol（IGMP）, Version 2
支持Protocol Independent Multicast-Sparse Mode (PIM-SM)
支持802.1x认证功能
支持PORTAL认证功能
支持Console 命令行配置
支持带内和带外端口的Telnet 命令行配置
支持Simple Network Management Protocol (SNMP)版本1，2和3
支持RMON 1，2，3，9组
支持带内和带外端口的WEB管理界面（Web-based Management）

1.3 虚拟局域网（VLAN）

VLAN（Virtual Local Area Network）又称虚拟局域网，VLAN是建立在物理网络基础上的一

种逻辑子网。一个VLAN组成一个逻辑子网，即一个逻辑广播域，它可以覆盖多个网络设备，允许处于不同地理位置的网络用户加入到一个逻辑子网中。建立VLAN需要相应的支持VLAN技术的网络设备。当网络中的不同VLAN间进行相互通信时，需要路由的支持，这时就需要增加路由设备——要实现路由功能，既可采用路由器，也可采用三层交换机来完成。

使用 VLAN 具有以下优点：

控制广播风暴，一个 VLAN 就是一个逻辑广播域，通过对 VLAN 的创建，隔离了广播，缩小了广播范围，可以控制广播风暴的产生。

提高网络整体安全性，VLAN 之间的访问只有通过三层路由转发才能实现，组网时同类属性的用户放在同一 VLAN，通过控制用户访问权限可以提高网络的安全性能。

组建和管理网络更加简单，有条理。

1.4 Spanning Tree Protocol（STP）

STP 在大的网络中定义了一个树，并且迫使一定的备份路径处于备用状态。如果生成树中的网络一部分不可达，或者 STP 值变化了，生成树算法会重新计算生成树拓扑，并且通过启动备份路径来重新建立连接。

STP 操作对于终端来说是透明的，而不管终端连在 LAN 的某一部分或者多个部分。

当创建网络时，网络中所有节点存在多条路径。 生成树中的算法计算出最佳路径。

STP 可以保证当在网络结构上存在冗余路径情况下，阻止网络回路状态发生，避免网络由于回路引发广播风暴，致使网络瘫痪，同时 STP 冗余链路可以使网络备份功能。

1.5 端口捆绑(Trunk)

Trunk可聚合多个端口成一逻辑端口，增加网络带宽，同时也使通道具有流量负载均衡能力以及系统容错能力。Trunk是一种廉价的提高带宽的办法，其成本是连接用的双绞线及占用端口。组成Trunk的物理端口通常应是同种类型的端口，如一般不会把千兆端口与百兆端口进行捆绑，而是千兆与千兆或百兆与百兆端口之间进行捆绑。

1.6 IGMP Snooping

IGMP 是路由器和它所连接的主机之间相互交换 IP 组播组信息的协议，有了 IGMP Snooping 功能，交换机能侦测经过它的 IGMP 报文，从中学习 IP 组播组信息,并将此学来的组播地址设置到交换机的侦听端口，使得传送下来的组播帧，仅转发给的这些端口。此项功能减少了不必要的网络带宽的浪费，同时便于开展 VOD,会议电视等组播视频应用。

1.7 DHCP Relay

DHCP Relay 可以在跨网段的情况下实现动态地址分配，即 DHCP 服务器与客户机可以不在相同的子网内，无须在每个子网内都放置 DHCP 服务器，各子网分支可以统一使用一个 DHCP 服务器来获取地址，便于大型网络的规划管理。

1.8 Qulity of Service (QoS)

通俗一点的说，QOS 是指针对某些指定的数据流量提供更好的服务的网络能力，可以通过提升流量队列的优先级来实现。QOS 可以使网络带宽资源得到有效的利用，为未来网络（包括数据，语音，视频）一体化提供基本条件，本系列交换机目前已经实现了端口优先级调度，802.1p 的 VLAN TAG 到优先级的映射，TOS 到优先级的映射等多项相关服务。

1.9 Access Control List (ACL)

访问控制列表（ACL）是提供系统访问安全性的一种有效策略。通过设置一系列许可或禁止规则来达到过滤控制的目的，本系列交换机控制策略非常丰富和灵活，可以基于源或目的 mac 地址、源或目的 IP 地址、协议类型及协议的源或目的端口等来制定，这些策略的的应用，并不降低数据转发的性能，系统仍能线速转发。

1.10 Mirroring

端口镜像（Mirroring）功能可以将一个端口的流量自动复制到另一端口，以供网络管理员在判断网络问题时对端口流量进行实时分析，可为网络管理人员提供一种监测手段。本系列交换机任何一个端口都可以配置成镜像端口。为了能使用网络分析仪直接监控网络流量，交换机必须支持端口镜像。

1.11 GARP VLAN Registration Protocol (GVRP)

GVRP 允许动态注册 802.1Q 的标记（tagged）VLAN,在需经过很多中间交换机进行通信的情况下，GVRP 非常有用，只要这些交换机均运行 GVRP,无须在每一台交换机配置 VLAN，便可实现通信。

1.12 GARP Multicast Registration Protocol (GMRP)

GMRP 用来动态注册 802.1Q 组播组，与 GVRP 有这相同的工作流程。

1.13 802.1x认证

IEEE 802.1x 称为基于端口的访问控制协议（Port based network access control protocol)。在 LAN 设备的物理接入级对接入设备进行认证和控制，连接在该类端口上的用户设备如果能通过认证，就可以访问 LAN 内的资源；如果不能通过认证，则无法访问 LAN 内的资源，相当于物理上断开连接。

IEEE 802.1x 协议的体系结构包括三个重要的部分：Supplicant System 客户端、Authenticator System 认证系统、Authentication Server System 认证服务器。

IEEE 802.1x 协议虽然源于 IEEE 802.11 无线以太网，但是，它在以太网中的引入，解决了传统的 PPPoE 认证方式带来的问题，消除了网络瓶颈，减轻了网络封装开销，降低了建网成本。

1.14 Portal认证

Web/Portal认证是基于业务类型的认证，不需要安装其他客户端软件，只需要浏览器就能完成，就用户来说较为方便。Web/Portal认证尤其适合在酒店等网络环境中使用。本

系列交换机对传统的Portal认证进行了改造，解决了传统不易检测用户是否离线的缺点，同时还做了许多其他优化处理，提高了效率、可靠性和易用性。

1.15 路由协议

通过将交换机的 VLAN 配置为虚拟的路由接口，在 VLAN 间进行相互访问时，需要通过三层路由。本系列交换机可以实现线速三层转发，路由表的建立支持静态配置和动态学习，目前支持以下动态路由协议：

路由信息协议 Routing Information Protocol (RIP) version 1

路由信息协议 Routing Information Protocol (RIP) version 2

开放式最短路优先协议 OSPF（Open Shortest Path Fist ）version 2

1.16 命令行管理

本系列交换机支持从Console口，Telnet方式的管理，Telnet可以通过带外口（AUX）访问，也可通过带内虚拟接口访问。命令行管理具有全部的配置和调试命令。

1.17 WEB管理

利用WEB浏览器界面管理交换机的功能。WEB可以通过带外口（AUX）访问，也可通过带内虚拟接口访问。WEB方式较为直观，但是其配置不是全部的配置集合，有些配置要在命令行部分才能完成。

1.18 SNMP

简单网络管理协议Simple Network Management Protocol（SNMP），利用SNMP，一个管理工作站可以远程管理所有支持这种协议的网络设备，包括监视网络状态、修改网络设备配置、接收网络事件警告等。本系列交换机支持SNMP版本1，2和3，并提供丰富的管理接口。

1.19 端口带宽管理

端口带宽管理用于管理每个端口的输入、输出带宽，可以对1至24端口的输入、输出速率进行配置。管理粒度为1M，管理粒度对不同的包长有一些误差，对512至1518字节长的包管理粒度比较准确，对64字节长的短包，1M会在1.3M左右。

第 2 章 管理交换机

本章主要介绍本系列交换机管理方式，管理风格，以及配置时需要了解的一些常识，内容包括：

- 选择管理方式
- 理解命令语法和风格
- 编辑命令
- 通用命令
- 升级内核
- 配置文件管理
- 系统重启动
- 保存配置
- 恢复出厂设置
- 检测网络基本连接
- ROM 启动模式
- 用户管理
- 配置带外管理口

2.1 选择管理方式

可以通过如下几种方法来管理本系列交换机:

- 终端或终端仿真软件通过计算机上串口COM和交换机的控制口（CONSOLE）相连，访问交换机的命令行接口（CLI）；
- TELNET方式，这可以通过带外管理接口（AUX），也可以通过配置带内虚拟接口管理。
- WEB浏览器方式，这可以通过带外管理接口（AUX），也可以通过配置带内虚拟接口管理。
- 基于SNMP的网管软件，这可以通过带外管理接口（AUX），也可以通过配置带内虚拟接口管理。
- 1个CONSOLE口连接,同时能支持5个TELNET连接。

2.1.1 使用CONSOLE口管理

可以通过在交换机前面面板上标有“CONSOLE”字样的 RJ-45 串口连接交换机内置的命令行。交换机 CONSOLE 端口的缺省配置如下：

波特率：9600

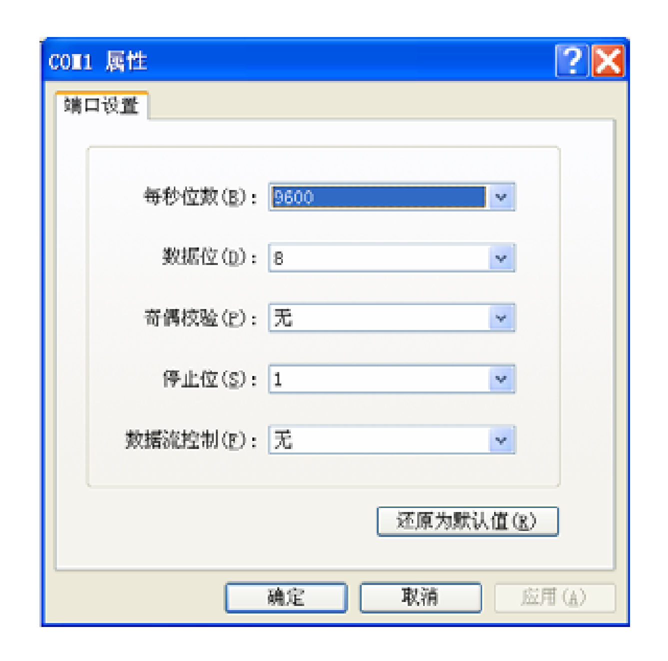
数据位：8

奇偶校验：无

停止位：1

流量控制：　无

因此用户应按下图参数来设置访问终端端口参数，同时建议用户使用VT100终端仿真。



如果连接成功，您就可以通过命令行接口对交换机进行配置了。

2.1.2 使用TELNET管理

若用户已经正确配置交换机接口的 IP 地址，这时可以用 telnet 远程登录到交换机，然后对交换机的命令行进行配置。交换机接口可以是带外管理接口（AUX 口），也可以是带内接口，如何配置 AUX 接口 IP 地址可参考“第 2 章”的 2.13 节，配置带内接口地址可参考“第 12 章”。

任何一个有 telnet 客户端功能的主机都能通过网络登陆到交换机，从而实现对交换机的配置管理。

【例如】在 Windows 操作系统的 DOS 模式下远程登录一台 IP 地址为 192.168.1.168 的交换机，可键入如下命令：

telnet 192.168.1.168

按回车，会出现如下信息，提示输入用户名字，输入用户名字后，例如 test，系统会提示输入密码，例如密码是 test，整个输入过程如下：

Login:　*test*

Password:　*test*

Switch>enable

Password:

若名字和密码正确通过认证，这时便进入系统的命令行配置状态。

☞　用 logout 命令可退出命令管理。

命令行方式（CLI）出厂缺省设置的用户名是 admin,无密码，在用户重新设置用户名

和密码后，该缺省设置失效。

AUX 接口出厂缺省设置的 IP 地址是 192.168.1.168,掩码是 255.255.255.0。

2.1.3 使用WEB管理

同 Telnet 接入一样，若用户已经正确配置交换机接口的 IP 地址，可用 WEB 浏览器对交换机进行管理。步骤如下：

第一步：配置交换机接口地址，如何配置 AUX 接口 IP 地址可参考“第 2 章”的 2.13 节，配置带内接口地址可参考“第 12 章”。

第二步：进行连接，将微机的以太网口通过局域网与交换机的以太网口连接。

第三步：打开 WEB 浏览器，输入交换机的地址，连通后，交换机会提示你键入用户名和密码，若正确输入用户名和密码后，即可进入 Web 页面进行管理。

☞ WEB 方式出厂缺省设置的用户名是 admin,密码是 password，在用户重新设置用户名和密码后，该缺省设置失效。

打开或者关闭 WEB 服务，利用命令：

switch(config)# ***webserver service*** *[enable|disable]*

如果选择enable表示打开WEB服务，选择disable表示关闭WEB 服务。

2.1.4 使用SNMP管理交换机

简单网络管理协议 SNMP(Simple Network Management Protocol)是一广泛使用的网管协议,帮助网管人员管理 TCP/IP 网络中各种装置,没有繁复的指令,概念上只有 fetch-store(存-取)两种命令,其优点为简单,稳定及灵活。

配置 SNMP 时，需要对以下参数进行了解：

Community：这一字符串提供了一个远程网络管理员配置交换机的用户确认机制。在交换机上有两种 Community 字符串。读确认 Community 字符串允许对交换机进行只读访问，缺省值为 public。读/写确认 Community 字符串提供了对交换机读/写操作的权限，缺省值为 private。

System Up Time：系统启动时间。

System contact：用于存放负责管理交换机的人名及联系方式。

System name：是指交换机指定的名称，方便记忆。

System location：这一个域是留给用户设置的，表示该交换机所在的位置。在交换机上，可以将 System location 设置为 The switch locates in room 101。

2.2 理解命令语法和风格

这一节主要介绍本系列交换机命令行语法风格，了解命令语法有利于配置的顺利进行。

2.2.1 分级用户保护模式

本交换机操作系统中，命令行提供两种用户模式，一为特权用户模式，另一为普通用户模式。这两种用户模式有不同的用户管理权限，特权用户有有着更大的管理权限，能执行所有配置命令，而普通用户只能查看其中的一些配置信息，不能进行配置。

用户以普通用户登入时，系统提示符为：

    hostname>

如为特权用户登入，则提示符为：

    hostname#

其中 hostname 可以在命令行更改，缺省为 switch。

系统共可设置 10 个用户，每个用户有自己的普通密码，如果为特权用户，还有自己的特权密码。若在登陆时，使用普通用户密码进入，系统就进入普通用户模式；若使用特权用户密码登陆，系统进入特权用户模式。特权用户以普通密码登入时只有普通用户权限，但可用 enable 命令并输入自己的特权密码进入特权模式。
普通用户模式进入特权用户模式，可以通过键入 enable 命令，具体命令操作如下：

switch>enable

回车后系统会提示输入特权用户密码

Password:

键入正确的特权用户密码后，可进入特权用户模式。

2.2.2 命令基本格式

命令为层次结构，由主节点直至叶结点，再到参数和可选参数，其格式为：
主节点　子节点 …　叶节点　参数 1 … 参数 n　[可选参数 1]…[可选参数 n]

【例如】switch(config)#　ip　　address　　add　　?
　　　　　　　　　　　子节点　　子节点　　叶结点　寻求帮助信息

屏幕将出现：
vint　Virtual interface to set.
系统提示输入虚接口，继续输入如：
switch(config)#　ip　address　add　vint ?
屏幕将出现：
<0-31>　Vint number.
系统提示输入虚拟接口的号码，继续输入如：
switch(config)#　ip　address　add　vint 1 ?
屏幕将出现：
<A.B.C.D>　Ip address set to the vint.
系统提示输入虚拟接口的 IP 地址，继续输入如：
switch(config)# ip add add vint 1 192.168.8.119 ?
屏幕将出现：
<A.B.C.D>　Subnet mask set to the vint.

系统提示输入子网掩码，继续输入如：

switch(config)# ip add add vint 1 192.168.8.119 255.255.255.0 ?

屏幕将出现：

vid Vlan set to the vint.

系统提示输入 vid，继续输入如：

switch(config)# ip add add vint 1 192.168.8.119 255.255.255.0 vid ?

屏幕将出现：

<1-4094> Vlan id.

系统提示输入 VLAN ID，继续输入如：

switch(config)# ip add add vint 1 192.168.8.119 255.255.255.0 vid 1 ?

屏幕将出现：

description Description to the vint.

<cr> Just Press <Enter> to Execute command!

系统提示输入 description 或直接回车，继续输入如：

switch(config)# ip add add vint 1 192.168.8.119 255.255.255.0 vid 1 description ?

屏幕将出现：

<string> STRING(1-20), description string

系统提示输入描述文字，继续输入如：

switch(config)# ip add add vint 1 192.168.8.119 255.255.255.0 vid 1 description test ?

屏幕将出现：

<cr> Just Press <Enter> to Execute command!

系统提示直接回车，结束命令：

- 左边一列出现的没有用<>括起来的参数的关键字，如第一个：vint 表示此参数关键字为 vint。
- 左边一列出现的用<>括起来的参数为对应关键字必选的参数，如第一个：<0-31>表示这是必选参数，范围在<0-31>之间。
- 右边一列为帮助信息，由[ ]括起来表示此参数是可选参数，如 [subnet mask]。
- <CR>表示在配完必选参数后，可以回车结束配置。

完整的命令为：

switch(config)#ip address add vint 1 192.168.8.119 255.255.255.0 vid 1 description test

【例如】switch(config)#ip address delete ?

屏幕将出现：

<A.B.C.D> Subnet ip address to delete.

左边一列由<>括起来表明此参数不带关键字，括号中的内容表明参数的格式。完整的命令为：

switch(config)#ip address delete 192.168.8.119

2.2.3 符号和参数类型说明

在命令语法中看到一些符号，这些符号只是规定了命令的配置使用方法，在使用时不应该把它作为命令一部分去输入，表 2-1 对这些符号进行了简要说明，表 2-2 对

参数类型进行了简要说明。

表 2-1 命令行符号列表

符　号	位　置	描　述
中括号[ ]	左列（即关键词参数列）	表示参数的类型。
中括号[ ]	右列（即帮助信息列）	若右列的帮助信息整项被括起，表示该配置项为可选项。
竖直线|	右列（即帮助信息列）	常与尖括号<>共同使用表示参数的可选项，例如<enable|disable>。
尖括号<>	右列（即帮助信息列）	参数的范围或可选项列表。

表 2-2 命令行参数类型列表

符　号	描　述
A.B.C.D	表示参数为 IP 地址，如 192.168.1.100。
Enum	表示参数为枚举类型，用户要在帮助信息列选其中的一个，如 enable|disable。
Mac-address	表示参数为物理地址，如 00:05:5D:E8:22:F0。
Num	表示参数为一数值。
String	表示参数为字符串，如 test。
<CR>	表示命令输入可以结束，即键入回车。

2.2.4 命令帮助

在对某个命令的语法不太确定的情况下，输入该命令中您所知道的前面的部分，然后键入“?”或“空格？”。

若键入“?”，命令行会提示所有可能的以已经输入部分开头的关键词，如输入下面的命令“a?”，系统会提示 access-list　arp authentication 三个可能的关键词，可根据所要配置的内容进一步选择关键词，例如配置 ACL， 可继续输入 access-list 关键词中余下的部分。

若输入“空格？”，命令行会提示该节点下所有子节点或参数。您就可以根据提示的命令继续输入命令，直至提示命令为再次出现以前的关键词时，表明命令输入完毕。按回车就可以执行所键入的命令。

2.2.5 命令简写

在输入命令时，您无须输入关键词的全部字母，而是只是关键字的前边部分字母，只要那部分字母不会造成歧义，系统就能够识别该命令。

【例如】创建标识为2的一条静态VLAN，其成员端口为端口2和15，键入命令：

```
switch(config)# vlan static add vid 2 02u15m
```

上述命令也可简写为： switch(config)# vl sta ad vid 2 02u15m

上述两条命令完成的功能相同。

注意：

当使用命令简写时，您必须输入足够多的字母，以确保在交换机的众多命令中不会造成歧义。

2.2.6 配置模式说明

交换机有以下几种命令行模式：

✧ RE（Readonly Exec）只读模式

该模式下只能查看一些普通信息，如版本号等。

系统提示符为：switch>

✧ GE（Global Exec）全局模式

该模式下能查看所有的配置信息，并提供如保存配置，重启动等一些系统命令。

在只读模式下键入enable命令，并正确输入超级用户密码可进入此模式，

系统提示符为：switch#

✧ CE（Configuration Exec)配置模式

该模式下提供各个功能模块配置命令。在全局模式下键入config命令，可进入此模式。

系统提示符为：switch(config)#

✧ 接口配置模式

在配置模式下键入interface vint <0-31>命令，可进入此模式。

系统提示符为：switch(config-if)#

✧ 路由配置模式

在配置模式下键入router ospf 命令，可进入此模式。

系统提示符为：switch(router-ospf)#

2.3 编辑命令

本节主要介绍系统命令行的编辑命令。

2.3.1 行编辑命令

在全局模式下输入命令 help edit，显示命令行界面编辑帮助如下，表 2-3 列出常用的行编辑命令：

```
Delete current character.....................Ctrl-d
Delete text up to cursor.....................Ctrl-u
Delete text after cursor.....................Ctrl-k
Move to beginning of line....................Ctrl-a
Move to end of line..........................Ctrl-e
Get prior command from history...............Ctrl-p
Get next command from history................Ctrl-n
Move cursor left.............................Ctrl-b
Move cursor right............................Ctrl-f
Move back one word...........................Esc-b
Move forward one word........................Esc-f
Convert rest of word to uppercase............Esc-c
Convert rest of word to lowercase............Esc-l
```

```
Delete remainder of word.....................Esc-d
Delete word up to cursor.....................Ctrl-w
Transpose current and previous character.....Ctrl-t
Enter command and return to root prompt......Ctrl-z
Refresh input line...........................Ctrl-l
```

表 2-3 常用的行编辑命令

符号	描述
BackSpace键或Del键或Ctrl+h	向左删除一个字符
向上箭头键或Ctrl+p	调用上一个历史命令
向左箭头键或Ctrl+b	将光标向左移动一格
向右箭头键或Ctrl+f	将光标向右移动一格
向下箭头键或Ctrl+n	如果前边使用过向上箭头调用上一个历史命令的，再单击向下箭头键可以显示下一个历史命令。
Ctrl+a	将光标移动到行首
Ctrl+e	将光标移动到行尾
Ctrl+d	将光标所在位置的字符删除
Ctrl+k	将光标以后的字符全部删除
Ctrl+t	将光标所在的字符和光标左边的那个字符互相调换，并将光标向右移动一格
Ctrl+u	整行删除
Ctrl+w	将光标左边的字符全部删除

2.3.2 显示暂停功能

在一次显示超过一屏时，系统提供了显示暂停功能，此时用户可以有三种选择，如表所示：

表 2-4 显示暂停按键列表

按　键	功　能
暂停显示时键入普通按键	继续显示下一屏信息
暂停显示时键入“q” 键	停止显示
暂停显示键入回车键	继续显示下一行信息

2.4 通用命令

2.4.1 内嵌命令

在全局模式下输入?，显示命令行内嵌的全局命令帮助如下：

```
Switch#?
  clear     Clear the screen.
```

```
config    Config system's setting.
debug     Debugging functions
download  Download file for software upgrade or load user config.
exit      Exit current mode and shift to previous mode.
help      Description of the interactive help system.
history   Config history command.
kill      Kill some unexpected things.
logout    Disconnect from switch and quit.
no        Negate a command or set its defaults.
ping      Ping command to test if the net is correct.
quit      Disconnect from switch and quit.
reboot    Reboot the switch.
remove    Remove from flash.
sendmsg   Send message to online user.
show      Show running system information.
terminal  Set terminal line parameters.
upload    Upload file for software upgrade or upload user config.
who       Display who is connected to the switch.
write     Save system info to flash.
```

向登录在线的管理用户发送消息

【命令】sendmsg sessionID *message*

〖命令模式〗全局模式

〖参数说明〗sessionID 可以通过who”命令查询；

“message” 指要发给用户的消息，消息不应有空格

〖使用导引〗 使用本命令前可用who命令查看哪些用户在线

〖参考举例〗

switch# who

系统提示：

```
SessionID  - UserName ---------- LOCATION ---------- MODE ----
3            admin          console         CONFIG     (That's me)
Total 1 sessions in current system
```

switch# sendmsg 3 hello,robbie!

系统提示：

admin(3): hello,robbie!

清空屏幕

【命令】clear

〖参数说明〗无参数

〖命令模式〗全局模式

〖 默认值 〗无

〖参考举例〗switch#clear

查看哪些管理用户在线

【命令】who
〖参数说明〗无参数
〖命令模式〗全局模式
〖 默认值 〗无
〖参考举例〗switch#who

退出现在的模式
【命令】exit
〖命令说明〗退出现在的模式，返回上一级模式，或返回根模式
〖参数说明〗无参数
〖命令模式〗所有模式都适用
〖 默认值 〗无
〖参考举例〗switch(config)#exit
switch#

退出系统状态
【命令】logout
〖参数说明〗无参数
〖命令模式〗全局模式
〖 默认值 〗无
〖使用导引〗使用该命令将关闭命令行的配置状态
〖参考举例〗switch#logout

2.4.2 常用命令

这一小节主要讲述命令行中常用的一些命令，特定功能的命令将在以后的章节专门讲述。

从普通用户模式转到配置模式
【命令】enable
〖参数说明〗无参数
〖命令模式〗普通模式
〖 默认值 〗无
〖参考举例〗Switch>enable
password:******

从特权用户模式转到普通用户模式
【命令】exit
〖参数说明〗无参数
〖命令模式〗全局模式
〖 默认值 〗无
〖参考举例〗Switch#exit
Switch>

从全局模式转到配置模式
【命令】config

〖参数说明〗无参数
〖命令模式〗全局模式
〖 默认值 〗无
〖参考举例〗Switch#config
Switch(config)

从配置模式转到接口配置模式
【命令】interface vint *<0-31>*
〖参数说明〗*<0-31>虚拟接口号*
〖命令模式〗配置模式
〖 默认值 〗无
〖参考举例〗switch(config)# int vint 0
switch(config-if)#

从配置模式转到路由配置模式
【命令】router ospf
〖参数说明〗*无*
〖命令模式〗配置模式
〖 默认值 〗无
〖参考举例〗switch(config)# router ospf
switch(router-ospf)#

显示系统版本信息
【命令】show version
〖参数说明〗无参数
〖命令模式〗只读模式，全局模式
〖 默认值 〗无
〖参考举例〗Switch#show version

显示过去用过的命令
【命令】history
〖参数说明〗无参数
〖命令模式〗所有模式
〖 默认值 〗无
〖参考举例〗Switch#history

显示系统配置信息
【命令】show running-config
〖参数说明〗无参数
〖命令模式〗只读模式，全局模式
〖 默认值 〗无
〖参考举例〗Switch#show running-config

改变系统命令行提示符
【命令】hostname *string*
〖参数说明〗string指新定义的提示符名字，不超过20个字符

〖命令模式〗配置模式
〖 默认值 〗系统缺省提示符是“Switch”
〖参考举例〗Switch(config)#hostname router
Router(config)#

设置系统时间
【命令】time <year> <month> <date> < hour： minute：second>
〖参数说明〗<year> 年
<month> 月
<date> 日
< hour： minute：second> 小时：分钟：秒

〖命令模式〗配置模式
〖参考举例〗
switch(config)# time 2002 8 21 11：55：0
用上述命令配置系统日期及时间为 2002 年 8 月 21 日 11 时 55 分 0 秒。

 用 show system config 命令显示配置是否成功。

2.5 升级内核

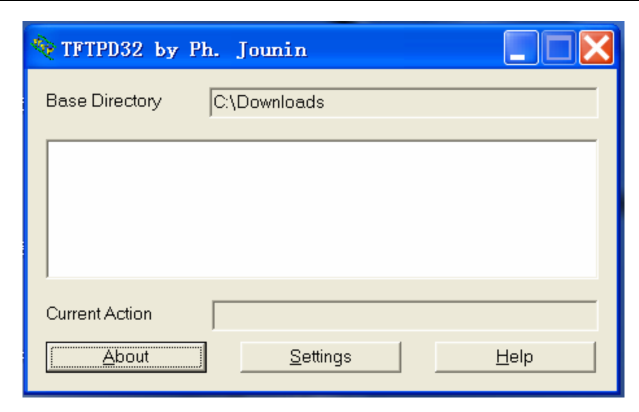
本节介绍升级系统内核的命令、方法及步骤。

2.5.1 升级命令

【命令】download tftp image <A.B.C.D> <filename>
〖命令说明〗升级交换机系统内核
〖参数说明〗<A.B.C.D> tftp服务器IP地址
<filename> 内核文件名字
〖命令模式〗全局模式
〖 默认值 〗无
〖使用导引〗参见下面的步骤
〖参考举例〗 switch# download tftp image 192.168.1.1 spros.z
其中 :192.168.1.98 是tftp服务器IP地址； spros.z 是内核文件名字

2.5.2 系统内核升级步骤

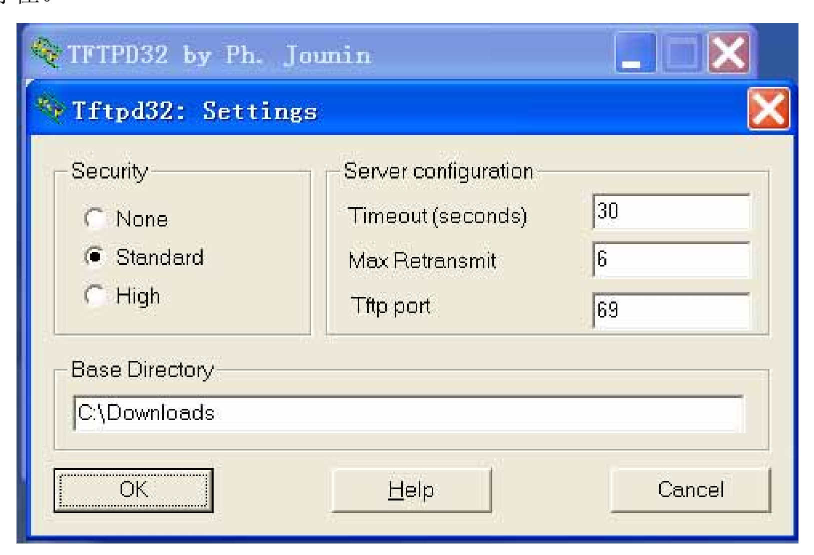
步骤 1：在 PC 上运行 Tftp Sever。



步骤 2：设置内核下载路径。

假如内核放在 C:\Downloads 目录下，可做如下设置。

点击 Settings 按钮，出现如下窗口，按图进行设置，Base Directory 为下载目录，注意下载目录要有内核存在。



步骤 3：连接主机网口与交换机的 AUX 口。

可直接对联（用交叉线），也可通过 SWITCH 或 HUB 连结（用直通线）。

步骤 4：启动交换机。

在命令行键入 show interface aux 命令，查看 aux 接口 IP 地址(如 192.168.1.168)，用 ping 命令确认此接口与主机可互通。若互通，继续下面的操作，否则检查网络连接是否连通。

步骤 5：下载操作。

```
switch# download tftp image 192.168.1.1 spros.z
```

步骤 6：耐心等待。

注意：

新内核成功下载到交换机后，重新启动系统后，这个新内核才能生效。

2.6 配置文件管理

本接主要介绍配置文件的管理，包括文件的上载和下载。

2.6.1 上载配置文件

【命令】upload tftp config <A.B.C.D> <filename>

〖命令说明〗从交换机上载配置文件到主机

〖参数说明〗<A.B.C.D> tftp服务器IP地址

<filename> 保存的配置文件名字

〖命令模式〗全局模式

〖 默认值 〗无

〖使用导引〗通过tftp下载，需有一台主机运行tftp server程序，步骤同2.5节升级内核。

〖参考举例〗 switch# upload tftp config 192.168.1.1 config

其中 :192.168.1.1 是tftp服务器IP地址； config 是备份的配置文件的名字

2.6.2 下载配置文件

【命令】 download tftp config <A.B.C.D> <filename>

〖命令说明〗下载配置文件到交换机

〖参数说明〗<A.B.C.D> tftp服务器IP地址

<filename> 配置文件名字

〖命令模式〗全局模式

〖 默认值 〗无

〖使用导引〗通过tftp下载，需有一台主机运行tftp server程序，步骤同2.5节升级内核。

〖参考举例〗 switch# upload tftp config 192.168.1.1 config

其中 :192.168.1.1 是tftp服务器IP地址； config 是配置文件的名字

注意：

配置文件成功下载到交换机后，系统重新启动后，新的配置才能生效。

2.7 系统重启动

【命令】reboot

〖命令说明〗重新启动系统

〖参数说明〗无参数

〖命令模式〗全局模式

〖 默认值 〗无

〖参考举例〗 Switch# reboot

注意：

在系统重启动前，请您确认是否需要保存配置，系统将丢失未保存的配置。

2.8 保存配置

【命令 1】 write

〖命令说明〗保存系统配置信息

〖参数说明〗无参数

〖命令模式〗全局模式

〖 默认值 〗无
〖参考举例〗 Switch# write

2.9 恢复出厂设置

【命令】remove
〖命令说明〗删除配置文件,下次启动时交换机会生成缺省配置的配置文件。
〖参数说明〗无参数
〖命令模式〗全局模式
〖 默认值 〗无
〖使用导引〗该命令将丢失所有您以前的配置信息，恢复到出厂设置
〖参考举例〗 Switch# remove

2.10 检测网络基本连接

【命令】ping *<A.B.C.D>*
〖命令说明〗测试网络通断情况
〖参数说明〗A.B.C.D指IP地址
〖命令模式〗全局模式
〖 默认值 〗无
〖参考举例〗

例 1：switch# ping 192.168.1.168

```
PING 192.168.1.168: 56 data bytes, press <Ctrl_D> to Stop.
Reply from 192.168.1.168: bytes=56 icmp_seq=0 ttl=64 time=0(ms)
Reply from 192.168.1.168: bytes=56 icmp_seq=1 ttl=64 time=0(ms)
Reply from 192.168.1.168: bytes=56 icmp_seq=2 ttl=64 time=0(ms)
Reply from 192.168.1.168: bytes=56 icmp_seq=3 ttl=64 time=0(ms)
Reply from 192.168.1.168: bytes=56 icmp_seq=4 ttl=64 time=0(ms)

PING 192.168.1.168 Statistics Info:
  5 packets transmitted, 5 packets received, 0% packet loss
  round-trip(ms) min/avg/max = 0/0/0
```

上述表示成功收到对方响应包，表示网络是连通的。

例 2：switch# ping 2.2.2.2

```
PING 2.2.2.2: 56 data bytes, press <Ctrl_D> to Stop.
Request time out.
Request time out.
Request time out.
Request time out.
Request time out.
PING 2.2.2.2 Statistics Info:
5 packets transmitted, 0 packets received, 100% packet loss
```

上述表示不能成功收到对方响应包，表示网络是不通的。

2.11 ROM启动模式

ROM模式是三层交换机启动时，首先进入的模式，若在提示的3秒钟内敲任何键则进入此模式，否则系统直接启动操作系统。
命令说明：

```
?        - print this list
b        - boot from basic operating system
c        - erase system config file
k        - erase system all kernel images
n        - boot from boot operating system
v        - show rom boot system version
```

“?” 显示帮助信息，在你不知道此模式下有什么命令，或想知道某条命令所执行的操作时，可使用此命令。
“b” 使系统从基本内核启动，在你的正常内核受到损坏时，使用此内核启动。
“c” 擦除系统配置文件，该命令一般不用，而且要慎用。
“k” 擦除全部系统内核，该命令一般不用，而且要慎用。
“n” 从正常系统内核启动。
“v” 显示rom boot系统版本。

注意：

在此模式，操作系统内核还没真正启动，此模式的某些操作属于非常底层的操作，如删除配置文件，系统内核等，因此使用时一定要慎重。

2.11 用户管理

2.11.1 添加用户

【命令 1】 user add *<username>* login-password *<login_password>*
〖参数说明〗*<username>*是所添加用户名字
*<login_password>*是普通用户登录密码，不少于6个字符
〖命令模式〗配置模式
〖参考举例〗
switch(config)#user add zhangsan login-password 123456
上述命令把 zhangsan 做为普通用户添加到系统，登录密码是 123456。

2.11.2 更改普通用户为超级用户

【命令 1】 use role *<username>* admin enable-password *<enable_password>*
〖参数说明〗*<username>*是已经存在的普通用户的名字
*<enable_password>*是超级用户登录密码，不少于6个字符
〖命令模式〗配置模式
〖参考举例〗

switch(config)# use role zhangsan admin enable-password 123456

上述命令把 zhangsan 由普通用户更改为超级用户，超级用户登录密码是 123456。

2.11.3 更改超级用户为普通用户

【命令 1】user role *<username>* **normal**

〖参数说明〗*<username>*是已经存在的超级用户的名字

〖命令模式〗配置模式

〖参考举例〗

switch(config)# use role zhangsan normal

上述命令把 zhangsan 由超级用户更改为普通用户

2.11.4 删除用户

【命令 2】user delete *<username>*

〖参数说明〗*<username>*是已经配置的用户名字

〖命令模式〗配置模式

〖参考举例〗 switch(config)#user delete zhangsan

上述命令把用户 zhangsan 删掉。

2.11.5 修改普通用户登录密码

【命令 3】user login-password *<username>*

〖参数说明〗*<username>*是已经存在的用户名字

〖命令模式〗配置模式

〖参考举例〗

switch(config)# user login-password zhangsan

系统提示：

Input new login password for user zhangsan please.

New Password:xxxxx

系统提示

Confirm Password:xxxxxx

系统提示

Successfully changed password!.

密码修改成功。

2.11.6 修改超级用户登录密码

【命令 3】user enable-password *<username>*

〖参数说明〗*<username>*是已经存在的用户名字

〖命令模式〗配置模式

〖参考举例〗

switch(config)# user enable-password zhangsan

系统提示：

Input new login password for user zhangsan please.

New Password:xxxxx

系统提示

Confirm Password:xxxxxx

系统提示

Successfully changed password!.

密码修改成功。

2.12 配置串口速率

【命令】serial speed *rate*

〖参数说明〗“rate”速率值，缺省是9600

〖命令模式〗配置模式

〖参考举例〗

1. switch(config)# *serial speed 9600*

   用上述命令配置系统串口速率为 9600。

2. switch# *show serial*

   上述命令显示系统串口速率信息。如：

```
Speed          :9600
Character size:8
Parity         :None
Stop Bits      :1
Flow Controll  :None
```

2.13 配置带外管理口(AUX)

设置 AUX 口的 IP 地址

【命令】interface aux ip set *<A.B.C.D>* *<X.X.X.X>*

〖参数说明〗*<A.B.C.D>*是 ip 地址

*<X.X.X.X>*是子网掩码

〖命令模式〗配置模式

〖参考举例〗

switch(config)# interface aux ip set 192.168.1.1 255.255.255.0

用上述命令设 AUX 口的地址为 192.168.1.1,掩码是 255.255.255.0。

删除 AUX 口的 IP 地址

【命令】interface aux ipaddress delete *<A.B.C.D>*

〖参数说明〗*<A.B.C.D>*是 ip 地址

〖命令模式〗配置模式

〖参考举例〗

switch(config)# interface aux ip delete 192.168.1.1

用上述命令删除 AUX 口的地址。

第 3 章 配置交换机端口

本章主要讲述如何配置交换机的端口。这些配置内容主要包括：

- 打开或关闭指定端口
- 打开或关闭指定端口的自适应功能
- 配置端口速度
- 配置端口的半双工或全双工模式
- 配置复用端口（21-24）的接口类型
- 配置端口的流控

3.1 端口基本参数配置

利用下面的命令进行端口的基本参数的设置。

打开或关闭端口

【命令 1】 port state 〈*portnumber*〉 enable|disable

〖参数说明〗enable|disable 表示端口使能与否；

〈*portnumber*〉表示所要设置的端口

〖命令模式〗配置模式

〖参考举例〗switch(config)# port state 20 enable

上述命令配置开启端口 20，并为其设置为全双工 100M 模式。

设置端口速率及模式

【命令 2】 port speed 〈*portnumber*〉 *rate*

〖参数说明〗rate 表示端口的速率：可以为

1000f　1000M full.

auto　auto.

〈*portnumber*〉表示所要设置的端口，其取值范围是 1-24。

〖命令模式〗配置模式

〖参考举例〗switch(config)# port speed 20 1000f

上述命令配置端口 20 为全双工 1000M 全双工模式。

设置复用端口类型

【命令 3】 port type 〈*portnumber*〉 *type*

〖参数说明〗tye 表示端口类型：可以为

copper　1000M 电口.

fiber　1000M 光口

〈*portnumber*〉表示所要设置的端口，其取值范围是 21-24。

〖命令模式〗配置模式

〖参考举例〗switch(config)# port type 21 fiber
上述命令配置端口 21 为光接口，这时电口 21 口不可用。

注意：

在关闭某端口时，要同时关闭该端口的spanning-tree参数,参见6.1.3节的【命令1】，如要关闭端口20，可运行下面的两个命令：

```
switch(config)#port state 20 disable
switch(config)# spanning-tree port 20 disable
```

WEB CONFIG 3.1-1



3.2 端口流控配置

打开端口流控

【命令 1】control flow *enable* port *<portnumber>*

〖参数说明〗enable 表示端口打开流控；
*<portnumber>*表示所要设置的端口，其取值范围是 1-24。

〖命令模式〗配置模式

〖参考举例〗switch(config)# control flow enable port 20
上述命令打开 20 口的流控功能。

关闭端口流控

【命令 2】control flow *disable* port *<portnumber>*

〖参数说明〗disable 表示端口关闭流控；
*<portnumber>*表示所要设置的端口，其取值范围是 1-24。

〖命令模式〗配置模式

〖参考举例〗switch(config)# control flow disable port 20
上述命令关闭端口 20 的流控功能

3.3 广播，组播和DLF抑制

起用广播抑制

【命令 1】control rate broadcast port *〈portnumber〉* **speed** *rate*

〖参数说明〗“rate”表示抑制速率，范围是 0-262143，值越小抑制作用越强，缺省值是 1024。
*〈portnumber〉*表示所要设置的端口，其取值范围是 1-24。
“broadcast”表示对广播包的抑制；
“*multicast*” 表示对组播包的抑制；
“dlf” 表示对 DLF 包的抑制，DLF 包是目的地址查找失败的包

〖命令模式〗配置模式

〖参考举例〗switch(config)# control rate broadcast port 12 speed 250
上述命令配置端口 12 对广播包的抑制速率是 250。

禁用广播抑制

【命令 2】control rate broadcast port *〈portnumber〉* **disable**

〖参数说明〗*portnumber〉*表示所要设置的端口，其取值范围是 1-24。

〖命令模式〗配置模式

〖参考举例〗switch(config)# control rate broadcast port 12 disable
上述命令关闭端口 12 对广播包的抑制。

起用组播抑制

【命令 1】control rate multicast port *〈portnumber〉* **speed** *rate*

〖参数说明〗“rate”表示抑制速率，范围是 0-262143，值越小抑制作用越强，缺省值是 256。
*〈portnumber〉*表示所要设置的端口，其取值范围是 1-24。
“broadcast”表示对广播包的抑制；
“*multicast*” 表示对组播包的抑制；
“dlf” 表示对 DLF 包的抑制，DLF 包是目的地址查找失败的包

〖命令模式〗配置模式

〖参考举例〗switch(config)# control rate multicast port 12 speed 250
上述命令配置端口 12 对组播包的抑制速率是 250。

禁用组播抑制

【命令 2】control rate multicast port *〈portnumber〉* **disable**

〖参数说明〗*portnumber〉*表示所要设置的端口，其取值范围是 1-24。

〖命令模式〗配置模式

〖参考举例〗switch(config)# control rate multicast port 12 disable
上述命令关闭端口 12 对组播包的抑制。

起用 DLF 抑制

【命令 1】control rate dlf port *〈portnumber〉* **speed** *rate*

〖参数说明〗“rate”表示抑制速率，范围是 0-262143，值越小抑制作用越强，缺省值是 256。

*<portnumber>*表示所要设置的端口，其取值范围是 1-24。

“dlf” 表示对 DLF 包的抑制，DLF 包是目的地址查找失败的包

〖命令模式〗配置模式

〖参考举例〗switch(config)# control rate dlf port 12 speed 250

上述命令配置端口 12 对 dlf 包的抑制速率是 250。

禁用 DLF 抑制

【命令 2】control rate dlf port *<portnumber>* disable

〖参数说明〗*portnumber>*表示所要设置的端口，其取值范围是 1-24。

〖命令模式〗配置模式

〖参考举例〗switch(config)# control rate broadcast port 12 disable

上述命令关闭端口 12 对 dlf 包的抑制。

☞ 在配置广播、组播的抑制时，speed 数值指每秒多少个包数，而与包的大小无关。例如，缺省值为 256，对 64 字节长的包对应速率为：256*64*8 bps,对 512 字节长的包对应速率为：256*512*8 bps。用户在配置的时候可参考 64 字节长的包 10M 标准速率为 14881，100M 准速率为 148810 的数值来设定。

在配置流控时，缺省配置数值为一般流控要求配置，FE 端口为 256，可满足个 2-4 个端口往一个端口发包时的流控要求，如要严格流控要求，如 20 个以上的端口往一个端口发包，则要减小配置值，FE 端口为 96。GE 端口一般是 FE 端口的 6 倍。数值越大流控越松，数值越小流控越严格。

3.4 端口带宽管理

本交换机的带宽管理（TAFFIC-LIMIT）可以基于物理端口设置，也基于访问控制列表设置，即对符合访问控制列表的特定数据流进行限速转发。下面将进行详细说明

3.4.1设置基于物理端口的带宽管理规则

3.4.1.1 定义基于物理端口带宽管理规则

【命令 1】traffic-limit link-group set *ruleid portlist* ingress <*ingress-rate* | default> egress <*egress-rate* | default>

〖参数说明〗

- ✧ “ruleid”表示规则号，取值范围是1 - 64 ，即最多可以设置64条限速条目。
- ✧ “portlist”：表示参与该访问控制列表的端口成员，以下方式输入 ：

  端口号+m

  例如02m15m，表示2端口和15端口为此条访问控制列表在其上生效的物理端口，注意上述命令的02 不要写成 2 。
- ✧ “ingress-rate”：表示最大入口速率值，范围是1-1023，粒度为1Mbits/S ；

"default"表示不限速。

✧ "egress-rate"：表示最大出口速率值，范围是1-1023，粒度为1Mbits/S ；"default"表示不限速。

〖命令模式〗配置模式

〖参考举例〗switch(config)# traffic-limit link-group set 1 01m02m ingress 2 egress 4

上述命令设置物理端口 01，02 的最大入口速率为 2 Mbits/S，最大出口速率为 4 Mbits/S 。

☞ 在设置基于物理端口的带宽管理时，应保证此带宽管理规则没有启用；如果已经有同一序号的带宽管理规则，则将会替换之。在全局模式下，用 show traffic-limit link-group *ruleid* 可查看是否设置成功。

3.4.1.2 使基于物理端口的带宽管理规则生效或失效

【命令 4】traffic-limit link-group <enable | disable> *ruleid*

〖参数说明〗

✧ "ruleid"表示规则号，取值范围是1 – 64 ，即最多可以设置64条限速条目。

✧ "enable"：使基于物理端口的带宽管理规则生效。

✧ "disable"：使用基于物理端口的带宽管理规则失效。

〖命令模式〗配置模式

〖参考举例〗switch(config)# traffic-limit link-group enable 2

上述命令使带宽管理规则 2 生效。

☞ 使基于物理端口的带宽管理规则生效或失效时，应保证此带宽管理规则必须已设置，否则将给予相应的提示信息。

3.4.1.3 删除基于物理端口的带宽管理规则

【命令 3】no traffic-limit link-group *ruleid*

〖参数说明〗"ruleid"表示规则号，取值范围是 1 - 64，该过滤规则必须已配置 。

〖命令模式〗配置模式

〖参考举例〗switch(config)#no traffic-limit link-group 2

上述命令删除带宽管理规则 2。

注意：在使基于物理端口的带宽管理规则生效或失效时，应保证此带宽管理规则必须已设置，否则将给予相应的提示信息。

3.4.2 设置基于访问控制列表的带宽管理规则

当访问控制列表为"permit"类型时，则可以对符合此条访问控制列表的数据流进行限速转发，即实现访问控制列表与带宽管理的捆绑；若此条访问控制列表为"deny"

类型，则由于符合此条访问控制列表的数据报都将被丢弃，故不必再对其进行限速转发处理，即便其与带宽绑定也没有任何效果。下面将详细说明如何设置基于访问控制列表的带宽管理规则。

3.4.2.1 定义基于访问控制列表的带宽管理规则

【命令 1】 traffic-limit acl-group set *acl-group* access-list ruleid *ruleid* ingress < *ingress-rate* | default>

〖命令说明〗定义一条基于访问控制列表 1 的带宽管理规则

〖参数说明〗

- ✧ “acl-group”是带宽管理规则的序号，取值范围为0-64 ；
- ✧ “ruleid”是访问控制列表的序号，表示此带宽管理规则与第几条访问控制列表绑定，取值范围是0-999 ；
- ✧ “ingress-rate” ：表示最大入口速率值，范围是1-1023，粒度为1Mbits/S ； “default”表示不限速。

〖命令模式〗配置模式

〖参考举例〗

```
switch(config)# traffic-limit acl-group set 1 access-list ruleid
            1 ingress 2
```

上述操作设置一条基于访问控制列表的带宽管理规则，其中，带宽管理规则号为 1 ，访问控制列表号是 1 ，符合此访问控制列表的数据流的最大入口速率为 2Mbit/s。

☞ 在设置基于访问控制列表的的带宽管理规则时，应保证此带宽管理规则没有启用；如果已经有同一序号的带宽管理规则，则将会替换之。在全局模式下，用 show traffic-limit acl-group *ruleid* 可查看是否设置成功并启用与否。

注意：在启用此条带宽管理规则前，应保证被绑定的访问控制列表已经启用，否则将给予相应的提示信息。

3.4.2.2 使基于访问控制列表的带宽管理规则生效或失效

【命令 4】 traffic-limit acl-group <enable | disable> *ruleid*

〖参数说明〗

- ✧ “ruleid”表示规则号，取值范围是1 - 64 ，即最多可以设置64条限速条目。
- ✧ “enable”：使基于访问控制列表的带宽管理规则生效。
- ✧ “disable”：使用基于访问控制列表的带宽管理规则失效。

〖命令模式〗配置模式

〖参考举例〗switch(config)# traffic-limit acl-group enable 2

上述命令使带宽管理规则 2 生效。

注意：在启用此条带宽管理规则前，应保证被绑定的访问控制列表已经启用，否则将给予相应的提示信息。

3.4.2.3 删除基于访问控制列表的带宽管理规则

【命令 3】no traffic-limit acl-group *ruleid*

〖参数说明〗“ruleid”表示规则号，取值范围是 1－64 ， 。

〖命令模式〗配置模式

〖参考举例〗switch(config)# no traffic-limit acl-group 2

上述命令删除带宽管理规则 2 。

☞ 在删除基于访问控制列表的带宽管理规则时，应保证此带宽管理规则已设置，否则将给予相应的提示信息。

第 4 章 配置 VLAN

VLAN（Virtual Local Area Network）又称虚拟局域网，VLAN是建立在物理网络基础上的一种逻辑子网。一个VLAN组成一个逻辑子网，即一个逻辑广播域，它可以覆盖多个网络设备，允许处于不同地理位置的网络用户加入到一个逻辑子网中。建立VLAN需要相应的支持VLAN技术的网络设备。当网络中的不同VLAN间进行相互通信时，需要路由的支持，这时就需要增加路由设备——要实现路由功能，既可采用路由器，也可采用三层交换机来完成。

使用 VLAN 具有以下优点：

- ✧ 控制广播风暴，一个 VLAN 就是一个逻辑广播域，通过对 VLAN 的创建，隔离了广播，缩小了广播范围，可以控制广播风暴的产生。
- ✧ 提高网络整体安全性，VLAN 之间的访问只有通过三层路由转发才能实现，组网时同类属性的用户放在同一 VLAN，通过控制用户访问权限可以提高网络的安全性能。
- ✧ 组建和管理网络更加简单，有条理。

4.1 VLAN端口成员类型

- **Port-Based VLAN 成员端口**

  Port-Based 端口将使从该端口发出去的 802.1Q 以态网帧去除 802.1Q 的帧标记而变成标准以态网帧，“u”代表此类型端口。

- **802.1Q Tagged VLAN 成员端口**

  802.1Q tagged 端口不改变发出去的以态网帧，“m”代表此类型端口。

4.2 配置说明

缺省 VLAN

每一台交换机出厂时都有一个缺省的 VLAN，该 VLAN 有以下属性：

- ✧ VLAN 的名字是 default
- ✧ 它包含所有端口
- ✧ default VLAN 的所有端口都是 untagged 的
- ✧ default VLAN 的 VLAN ID 是 1

符号解释

在配置 VLAN 时，常用到以下符号，说明如下：

“-” 代表此端口不属于这个 VLAN。

“u”代表此端口是这个 VLAN 的 untagged 成员。

“m”代表此端口是这个 VLAN 的 tagged 成员。

4.3 配置静态VLAN

4.3.1 添加一条静态VLAN

实现添加一条静态 VLAN，需要执行以下几条命令。

【命令1】vlan static add vid *Num String*

〖参数说明〗参数包括要添加VLAN的ID“Num”以及端口成员参数“String”，“Num”是1~4094之间的整数。端口成员参数“String”按以下方式输入：

端口号+端口类型

例如02u15m，表示2端口为这个VLAN的untagged成员，15端口为该VLAN的tagged成员。注意上述命令的02不要写2。

〖命令模式〗配置模式

〖参考举例〗 switch(config)# vlan static add vid 2 01m08u19m

上述操作将 1,8 和 19 端口归到 vlan 2 中,其中 1 和 19 端口是 802.1 tagged 方式的成员端口，8 端口是 untagged 方式。注意上述命令的 01 和 08 不要写为 1 和 8。

WEB CONFIG 4.3.1-1



【命令 2】vlan port pvid *portnum pvlanid*

〖命令说明〗设置端口VLAN PVID值，用于untagged包的标记，以决定其走哪个VLAN。

〖参数说明〗参数包括端口成员号“portnum”和该端口的PVID值“pvlanid”。“portnum”是1~24之间的整数；“pvlanid”应该是该端口上配置的某个VLAN ID值，并且该VLAN ID必须是已经存在的。

〖命令模式〗配置模式

〖参考举例〗

switch(config)# *vlan port* pvid 1 2

switch(config)# *vlan port* pvid 8 2

switch(config)# *vlan port* pvid 19 2

上述三条命令设置成员 1，8 和 19 端口的 PVID,均设为 2。

WEB CONFIG 4.3.1-2



虚拟局域网(VLAN)

VLAN 列表 | 静态VLAN 配置 | GVRP 状态 | VLAN/GVRP 端口

VLAN 端口选择			
单元号	1	端口号	1

端口	优先级	PVID	接收侦选择	输入过滤控制	GVRP使能	注册失败计数	最新PDU源地址
1	0	2	all	disable	enable	0	00:00:00:00:00:00
1	0	2	all	disable	enable	0	00:00:00:00:00:00
2	0	2	all	disable	enable	0	00:00:00:00:00:00
3	0	1	all	disable	enable	0	00:00:00:00:00:00
4	0	1	all	disable	enable	0	00:00:00:00:00:00
5	0	1	all	disable	enable	0	00:00:00:00:00:00

【命令 3】show vlan table

〖命令说明〗查看 VLAN 的静态端口成员

〖参数说明〗无参数

〖命令模式〗全局模式

〖参考举例〗switch# show vlan table 查看刚才加的 VLAN 是否成功

WEB CONFIG 4.3.1-3



虚拟局域网(VLAN)

VLAN 列表 | 静态VLAN 配置 | GVRP 状态 | VLAN/GVRP 端口

VLAN 单元选择	
单元号	1

VID	FID	状态	1 8	9 16	17 24
1	1	Static	U - - - - - - -	- - - - - - - -	- - - - - - - -
2	1	Static	- U - - - - - -	- - - - - - - -	- - - - - - - -
3	1	Static	- - U - - - - -	- - - - - - - -	- - - - - - - -
4	1	Static	- - - U - - - -	- - - - - - - -	- - - - - - - -
5	1	Static	- - - - U - - -	- - - - - - - -	- - - - - - - -

[提示] -=None M=Member U=Untagged

刷新

【命令 4】show vlan port [<1-24>]

〖命令说明〗查看端口 pvid 值

〖参数说明〗[<1-24>]，可选参数，表示选定的端口

〖命令模式〗全局模式

〖参考举例〗switch# show vlan port 1

4.3.2 删除一条静态VLAN

【命令1】vlan static delete vid *num*

〖参数说明〗“Num”是已经存在的VLAN号，是1~4094之间的整数。

〖命令模式〗配置模式

〖参考举例〗switch(config)# vlan static delete vid 2

上述操作将 VLAN 2 删除。

注意：

删除操作必须对已经存在的VLAN,进行，删除不存在的VLAN时，系统会报错。

用 show vlan table 查看是否删除成功。

WEB CONFIG 4.3.2-1



4.3.3 修该静态VLAN的成员端口

【命令1】vlan static set vid *Num String*

〖参数说明〗参数包括要修改VLAN的ID“Num”以及端口成员参数“String”,

“Num”是1~4094之间的整数。端口成员参数“String”按以下方式输入：

端口号+端口类型

例如02u15m，表示2端口为这个VLAN的untagged成员，15表示该VLAN的tagged成员。注意上述命令的02不要写2。

〖命令模式〗配置模式

〖参考举例〗switch(config)# vlan static set vid 3 01m08u03-

上述操作将 1 端口设为 VLAN 3 的 802.1 tag 方式的成员端口，8 端口

设为 untag 方式的成员端口，“03-” 表示把 3 端口从 VLAN 的成员中删除。注意上述操作对原 VLAN 3 的其他成员端口不影响。

注意：

操作必须对已经存在的VLAN,进行，修改不存在的VLAN时，系统会报错。

☞ 用 show vlan table 查看是否修改成功。

4.4 动态VLAN

打开或关闭 GVRP 协议

【命令1】system gvrp <*enable/disable*>

〖参数说明〗 enable表示打开动态VLAN注册协议（GVRP），disable表示关闭此协议。
〖命令模式〗配置模式
〖参考举例〗

- 打开动态 VLAN 开关

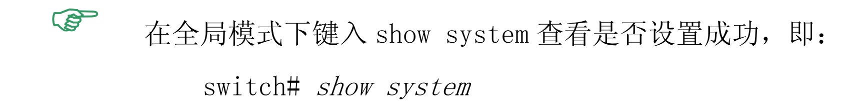
```
switch(config)# system gvrp enable
```

上述操作打开动态 VLAN 注册协议。

- 关闭动态 VLAN 开关

```
switch(config)# system gvrp disable
```

上述操作打开动态 VLAN 注册协议。



☞ 在全局模式下键入 show system 查看是否设置成功，即：

switch# *show system*

WEB CONFIG 4.4-1



配置端口允许或禁止参加动态注册 VLAN

【命令2】vlan port gvrp *portnum* <*enable*|*disable*>

〖参数说明〗“portnum”表示参加此操作端口号，范围为1-24；
enable表示该端口允许VLAN注册，disable表示不允许此协议。
〖命令模式〗配置模式
〖参考举例〗switch(config)# vlan port gvrp 2 disable
上述操作禁止端口 2 参加动态 VLAN 注册

WEB CONFIG 4.4-2

虚拟局域网(VLAN)

VLAN 列表 | 静态VLAN 配置 | GVRP 状态 | VLAN/GVRP 端口

VLAN 端口选择			
单元号	1	端口号	1

端口	优先级	PVID	接收帧选择	输入过滤控制	GVRP使能	注册失败计数	最新PDU源地址
1	0	2	all	disable	enable	0	00:00:00:00:00:00
1	0	2	all	disable	enable	0	00:00:00:00:00:00
2	0	2	all	disable	enable	0	00:00:00:00:00:00
3	0	1	all	disable	enable	0	00:00:00:00:00:00

4.5 配置SUPERVLAN

4.5.1 创建一个新的supervlan实体

【命令1】supervlan create supervlan *Index* mastervlan *Num* subvlan *string*

〖参数说明〗参数*Index*是supervlan的序号，取值范围1－5。参数*Num*是主vlan号，是1~4094之间的整数。参数String指定子vlan成员，按以下方式输入：
vlan号 + m
例如2m3m，指定vlan2、vlan3为该supervlan的子vlan。

〖命令模式〗配置模式
〖参考举例〗switch(config)#supervlan create supervlan 1 mastervlan 1 subvlan 2m3m
以上操作创建一条包含 vlan1、2、3 的 supervlan 其中 vlan1 为主 vlan。

在全局模式下键入 show supervlan 查看是否设置成功，即：

switch# *show supervlan*

注意：

只有主 vlan 可以有 ip 子网地址，其它子 vlan 成员不能有 ip 子网地址。并且一定要保证 supervlan 中的主 VLAN 一定要配置 IP 地址。

4.5.2 添加子vlan到supervlan

【命令1】supervlan addsub supervlan *Index* subvlan *string*

〖参数说明〗参数*Index*是supervlan的序号，取值范围1－5。参数String指定要添加的子vlan成员，按以下方式输入：vlan号 + m

例如2m3m，指定添加vlan2、vlan3为该supervlan的子vlan。

〖命令模式〗配置模式

〖参考举例〗switch(config)# supervlan addsub supervlan 1 subvlan 2m3m

以上操作添加 vlan2、3 到 supervlan1 中去。

在全局模式下键入 show supervlan 查看是否设置成功，即：

switch# *show supervlan*

注意：

添加的子vlan成员不能有ip子网地址。

4.5.3 删除子supervlan的子vlan 成员

【命令1】supervlan delsub supervlan *Index* subvlan *string*

〖参数说明〗参数*Index*是supervlan的序号，取值范围1－5。参数String指定要删除的子vlan成员。

〖命令模式〗配置模式

〖参考举例〗switch(config)# supervlan delsub supervlan 1 subvlan 03m

以上操作将 vlan3 从 supervlan1 中删除。



在全局模式下键入 show supervlan 查看是否设置成功，即：

switch# *show supervlan*

4.5.4 删除supervlan

【命令1】supervlan delete supervlan *Index*

〖参数说明〗参数*Index*是supervlan的序号，取值范围1－5。

〖命令模式〗配置模式

〖参考举例〗switch(config)# supervlan delete supervlan 1

以上操作删除 super1vlan1。



在全局模式下键入 show supervlan 查看是否设置成功，即：

switch# *show supervlan*

4.6 其它配置

帧类型过滤

通过下面的设置可以使端口允许或禁止非 802.1Q Tagged 帧进入交换机。

【命令1】vlan port frame *portnum <all/tagged-only>*

〖参数说明〗“portnum”表示参加此操作端口号；

“all”表示该端口允许所有帧进入，“*tagged -only*”表示只允许 VLAN Tagged帧进入。

〖命令模式〗配置模式

〖参考举例〗switch(config)# vlan port frame 2 tagged-only

上述操作端口 2 只允许 VLAN Tagged 帧进入

WEB CONFIG 4.6-1

虚拟局域网(VLAN)

VLAN 列表 | 静态VLAN 配置 | GVRP 状态 | VLAN/GVRP 端口

VLAN 端口选择			
单元号	1	端口号	1

VLAN/GVRP 端口配置							
端口	优先级	PVID	接收帧选择	输入过滤控制	GVRP使能	注册失败计数	最新PDU源地址
1	0	2	all	disable	enable	0	00:00:00:00:00:00
1	0	2	all	disable	enable	0	00:00:00:00:00:00
2	0	2	all	disable	enable	0	00:00:00:00:00:00
3	0	1	all	disable	enable	0	00:00:00:00:00:00

帧转移过滤

当交换机的某个端口收到的802.1Q Tagged帧不是自己所属的VLAN时，交换机可以允许或禁止将收到的帧转移到交换机内该帧标识的VLAN去。例如端口4被配置成只属于VLAN 1，端口5被配置成只属于VLAN 2，若端口4收到标识为VLAN2的帧，交换机可以配置成将该帧转移到端口5。

【命令2】vlan port filter *portnum <enable/disable>*

〖参数说明〗“portnum”表示参加此操作端口号；

enable表示该端口不允许帧转移，disable表示允许帧转移，系统缺省是disable。

〖命令模式〗配置模式

〖参考举例〗switch(config)# vlan port filter 2 enable

上述操作不允许端口 2 帧转移。

第 5 章 FDB 表

交换机根据收到的数据帧的源 MAC 地址进行表项学习，建立一张 MAC 地址，端口以及 VLAN 的映射表，该表通常叫做交换机的物理地址表，也叫转发数据表 FDB（Forward DataBase），当交换机收到一帧数据时，它将根据数据帧目的 MAC 查找自己 FDB 表来决定该数据帧从哪个端口转发。

每个 FDB 地址表项都包含以下内容：

- ✧ MAC 地址
- ✧ 与 MAC 地址关联的端口号（Port）
- ✧ 与 MAC 地址关联的 VLAN 的名称(Vlan name)
- ✧ 该 FDB 地址表项的标志(Flags)

5.1 配置FDB表

系统提供配置物理地址的老化时间。

【命令 1】fdb agingtime *number*

〖参数说明〗“number”MAC地址老化时间，单位是秒，范围是10-1000000，缺省值是300
〖命令模式〗配置模式
〖参考举例〗switch(config)# fdb agingtime 200

5.2 显示FDB表

显示 FDB 地址老化时间

【命令 1】show fdb agingtime

〖参数说明〗无
〖命令模式〗全局模式
〖参考举例〗switch# show fdb agingtime

按端口显示 FDB 表

【命令 1】show fdb port *number*

〖参数说明〗“number”表示端口号，范围是1-24
〖命令模式〗全局模式
〖参考举例〗switch# show fdb port 2
系统显示：

```
.........mac address table information on port 2.......
    index      mac-address       vlan-id  port     flags
    1        00:de:b0:10:82:00        1      2      age
```

按 VLAN 显示 FDB 表

【命令 1】show fdb vlan *number*

〖参数说明〗 "number"表示vlan号.
〖命令模式〗 全局模式
〖参考举例〗 switch# show fdb vlan 2
系统显示：

```
.........mac address table information on vlan 1.......

index      mac-address       vlan-id    port     flags

  1      00:00:00:00:00:00        2       1      static|routed

  2      00:de:b0:10:81:00        2       1      age

  3      00:de:b0:10:82:00        2       2      age

  4      00:de:b0:10:83:00        2       3      age
```



上面 flag 的几个选项解释如下：
static 表示静态存在的，是不能被老化的
routed 表示该表项用于三层路由转发，是不能被老化的
age 表示正常学到的二层转发表，会老化

第 6 章 STP 协议

STP 可以保证当在网络结构上存在冗余路径情况下，阻止网络回路状态发生，提供了网络的动态冗余切换机制，避免网络由于回路引发广播风暴，致使网络瘫痪，同时 STP 冗余链路可以使网络备份功能。交换机支持 IEEE802.1D 标准的 STP 协议。

6.1 配置STP

在交换机上配置 STP 包含以下内容：

✧ 打开或关闭 STP 开关

✧ 设置 STP 桥的参数

✧ 设置端口生成树参数

6.1.1 打开或关闭STP开关

交换机中 STP 缺省状态是关闭的。设定的 STP 开启和关闭，利用命令：

【命令1】system span *<enable/disable>*

〖参数说明〗enable表示开启STP开关，disable表示关闭STP开关。
〖命令模式〗配置模式
〖参考举例〗

- 开启生成树开关
  switch(config)# system span enable
  上述操作打开生成树协议开关。

- 关闭生成树开关
  switch(config)# system span disable
  上述操作关闭生成树协议开关。

☞ 在全局模式下键入 show system 查看是否设置成功，即：

switch# show system

🎬WEB CONFIG 6.1.1-1

生成树协议(STP)

协议状态设置 | STP 桥参数 | STP 端口参数

STP 协议状态设置	
生成树协议开关	disable

6.1.2 设置STP桥的参数

系统运行 STP 协议后，您可能需要根据具体的网络结构调整该 STP 的一些桥参数。这些参数包括：

- ✧ Bridge Priority
- ✧ Hello Time
- ✧ Forward Delay
- ✧ Max Age

下面分别介绍设置上述参数的配置命令。

【命令1】 spanning-tree bridge priority *num*

〖命令说明〗设置运行STP协议时本交换机的优先级

〖参数说明〗优先级值“num”的取值范围是 0-65535，缺省值为 32768。
优先级数值越低，越有可能成为网络中的根桥（Root Bridge）。优先级值为 0 代表了最高的优先级。

〖命令模式〗配置模式

〖参考举例〗switch(config)# spanning-tree bridge priority 32769
上述操作把本机生成树协议优先级设为 32769。

【命令2】 spanning-tree bridge hellotime *num*

〖命令说明〗设置当本交换机被选为根桥时发送 BPDU 的时间间隔。

〖参数说明〗HelloTime 值“num”的取值范围是 100-1000，单位为百分之一秒，缺省值是 200。

〖命令模式〗配置模式

〖参考举例〗 switch(config)# spanning-tree bridge hellotime 200
上述操作把生成树协议 hello time 间隔设为 2 秒

【命令3】 spanning-tree bridge Forward *num*

〖命令说明〗设置当本交换机被选为根桥时端口状态切换的时间间隔
〖参数说明〗ForwardDelay参数值“num”的取值范围是400-3000，单位为百分之一秒，缺省值为1500
〖命令模式〗配置模式
〖参考举例〗switch(config)# spanning-tree bridge forword 1500
上述操作把生成树协议转发延迟设为 15 秒

注意：

Forward的时间必须大于等于HelloTime+200

【命令4】 spanning-tree bridge agingtime *num*

〖命令说明〗设置 BPDU 报文老化的最长时间间隔，如果收到超过这个时间的 BPDU 报文，就直接丢弃。
〖参数说明〗agingtime参数值“num”的取值范围是600-4000，单位为百分之一秒，缺省值为2000
〖命令模式〗配置模式
〖参考举例〗switch(config)# spanning-tree bridge agingtime 2000
上述操作把生成树协议最大老化时间设为 20 秒。

注意：

agingtime的时间必须大于等于2*(HelloTime＋100)，小于等于2*(ForwardDelay － 100)

在全局模式下，用 show spanning-tree bridge 查看是否设置成功，即 switch# show spanning-tree bridge。

WEB CONFIG 6.1.2-1

生成树协议(STP)

协议状态设置 | STP 桥参数 | STP 端口参数

STP 桥参数	
STP 委派根参数	0000 00:00:00:00:00:00
优先级	32768
Hello 间隔时间	200
转发延迟	1500
最大老化时间	2000
Root 端口	0
Root 开销	0
拓扑更改次数	0

6.1.3 设置端口生成树参数

端口生成树参数主要有以下两个参数，分别介绍如下：

【命令 1】 spanning-tree port *num* *<enable/disable>*

〖命令说明〗允许/禁止某端口参与生成树计算

〖参数说明〗端口号参数值“num”的取值范围是 1-24， enable 表示该端口参与 STP 计算，disable 表示不 STP 参与 STP 计算

〖命令模式〗配置模式

〖参考举例〗switch(config)# spanning-tree port 2 enable

上述操作使生成树协议在端口 2 上起作用。

☞ 在全局模式下，用 show spanning-tree ports 查看是否设置成功，即

switch# show spanning-tree ports

WEB CONFIG 6.1.3-1



【命令 2】 spanning-tree port *portnum* priority *num*

〖命令说明〗配置参与 STP 计算的端口的优先级

〖参数说明〗端口号参数值“portnum”的取值范围是 1-24，端口优先级“num”的取值范围是 0-255，缺省值是 128。优先级数值越低，端口越容易成为根端口（Root Port），优先级值为 0 代表了最高的优先级。

〖命令模式〗配置模式

〖参考举例〗 switch(config)# spanning-tree port 2 priority 20

上述操作使生成树协议在端口 2 具有优先级 20。

☞ 在全局模式下，用 show spanning-tree ports 查看是否设置成功，即

switch# show spanning-tree ports

WEB CONFIG 6.1.3-2

生成树协议(STP)

协议状态设置 | STP 桥参数 | STP 端口参数

STP 端口选择			
单元号	1	端口号	1

STP 端口参数					
桥端口	使能设置	路径开销	优先级	转发变换次数	状态
1	enable	19	128	1	forwarding
1	enable	19	128	1	forwarding
2	enable	10	128	1	forwarding
3	enable	10	128	1	forwarding

第 7 章 配置组播

组播技术适用于多点到多点或一点到多点的数据传输业务，组播强制网络在数据流分布树的分叉处进行信息包复制，而不是由信息源节点多次重复地发送相同的数据包，交换机完成网络末端组播包的透明传递和分发，降低了信息源的性能要求，优化了网络数据流量。

7.1 静态组播

本交换机支持静态配置组播组。本节主要介绍静态组播的配置方法。

7.1.1 添加一条静态组播

【命令1】multicast-group static add vid *vidnum macaddr portstring*

〖命令说明〗配置一条静态组播组项

〖参数说明〗vidnum参数值“vidnum”的取值范围是1-4095，而且必须是已经存在的VLAN号；macaddr是组播物理地址，是一些以01开头的组播物理地址，但不包括01:00:5e开头的这段地址，01:00:5e开头的这段地址由igmp-snooping协议添加、更改和删除，端口成员参数“portstring”按以下方式输入：

端口号+(m或-)

例如02m15m，表示2端口和15端口为这个组播组成员，注意上述命令的02不要写2。

〖命令模式〗配置模式

〖参考举例〗

switch(config)#multicast-group static add vid 2 01:00:23:21:03:02 08m11m

上述操作将 VLAN 2 的成员端口 8 和 11 设置为组播地址为 01:00:23:21:03:02 的组播成员。

注意：

上述操作中，成员端口必须属于同一 VLAN，同时所配的 mac 组播地址必须是 01 开头，并且不是保留的组播地址，如：01:00:5e:xx:xx:xx，01:80:C2:00:00:xx 等。

在全局模式下，用 show multicast-group 查看是否设置成功，即

switch# show multicast-group

WEB CONFIG 7.1-2

组播(Multicast)

组播组列表 组播组配置 GMRP 状态 GARP/GMRP 端口

单元选择	
单元号	1

组播组配置				
VID	组播 Mac地址	1 8	9 16	17
1	01:00:12:20:ea:11	M M M - - - - -	- - - - - - - -	- - - -
0001 01:00:12:20:ea:11	[提示] -=非成员 M=成员 F=禁止成员			

7.1.2 删除一条静态组播

【命令1】multicast-group static delete vid *vidnum macaddr*

〖命令说明〗删除一条静态组播组项

〖参数说明〗 vidnum参数值“vidnum”的取值范围是1-4095，而且必须是已经存在的VLAN号；macaddr是组播物理地址，是一些以01开头的组播物理地址，但不包括01:00:5e开头的这段地址，01:00:5e开头的这段地址由igmp-snooping协议添加、更改和删除 。

〖命令模式〗配置模式

〖参考举例〗switch(config)#multicast-group static delete vid 2 01:00:23:21:03:02

上述操作将删除组播地址为 01:00:23:21:03:02 的组播群

注意：

上述删除操作中，该组播组必须是存在的，否则系统会报错。

在全局模式下，用 show multicast-group 查看是否设置成功，即

switch# show multicast-group

WEB CONFIG 7.1-2

组播(Multicast)

组播组列表 | 组播组配置 | GMRP 状态 | GARP/GMRP 端口

单元选择	
单元号	1

组播组配置				
VID	组播 Mac地址	1 … 8	9 … 16	17 …
1	01:00:12:20:ea:11	M M M - - - - -	- - - - - - - -	- - -
0001 01:00:12:20:ea:11	[提示] -=非成员 M=成员 F=禁止成员			

刷新 应用 删除

7.2 通用组播注册协议GMRP

GMRP 用来动态注册 802.1Q 组播组，与通用 VLAN 注册协议 GVRP 有这相同的工作流程。

【命令1】system gmrp *<enable/disable>*

〖命令说明〗打开和关闭GMRP协议

〖参数说明〗enable表示打开动态组播注册协议，disable表示关闭此协议。

〖命令模式〗配置模式

〖参考举例〗

- 打开动态组播开关

  switch(config)# system gmrp enable

  上述操作打开动态组播注册协议。

- 关闭动态组播开关

  switch(config)# system gmrp disable

  上述操作关闭动态组播注册协议。



在全局模式下键入 show systemconfiguration 查看是否设置成功，即：

switch# show system configuration

WEB CONFIG 7.2-1

组播(Multicast)

组播组列表 | 组播组配置 | GMRP 状态 | GARP/GMRP 端口

GMRP 状态设置	
GMRP 使能状态	disable

7.3 IGMP Snooping

IGMP Snooping 通过监听三层 IGMP 协议的 Report 和 Leave 报文来实现组播组的动态添加和删除，实现网络末端组播包的透明传递和分发。

开启/关闭 igmp-snooping 协议

【命令1】system igmp-snooping <*enable*|*disable*>

〖命令说明〗打开和关闭igmp-snooping协议
〖参数说明〗enable表示打开协议，disable表示关闭此协议。
〖命令模式〗配置模式
〖参考举例〗

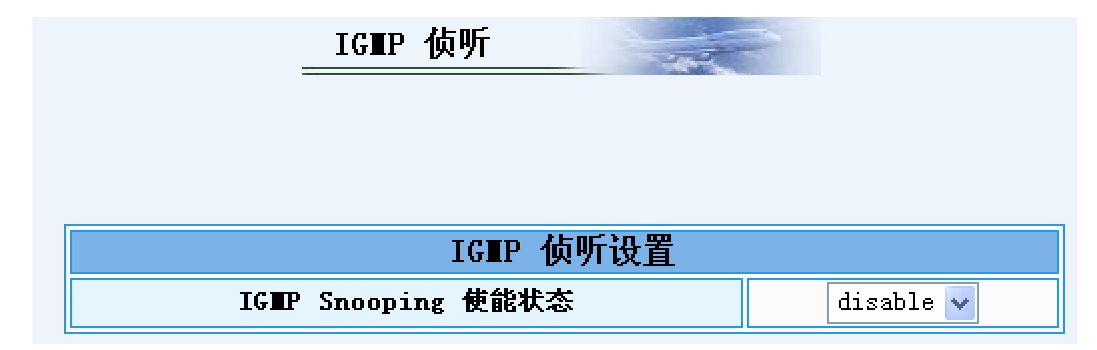
- 打开 igmp-snooping 协议
  switch(config)# system igmp-snooping enable
- 关闭 igmp-snooping 协议
  switch(config)# system igmp-snooping disable



在全局模式下键入 show system configuration 查看是否设置成功，即：

switch# show system configuration

WEB CONFIG 7.3-1



删除组播组

【命令2】igmp-snooping clean *vidnum*

〖命令说明〗基于VLAN ID删除组播组成员
〖参数说明〗“vidnum”VLAN号,必须是已经配置的vlan号，0表示全部VLAN
〖命令模式〗配置模式
〖参考举例〗switch(config)# igmp-snooping clean 2

 在全局模式下键入 show igmp-snooping vlan *vidnum* 查看是否设置成功，如：

switch# show igmp-snooping vlan 2

设置组播组

【命令1】igmp-snooping timeout *time*
〖命令说明〗设置igmp-snooping学来的组播组老化时间
〖参数说明〗“time”老化时间值，取值范围在30-3600秒,缺省值300秒
〖命令模式〗配置模式
〖参考举例〗switch(config)# igmp-snooping timeout 200

☞ 在全局模式下键入 show igmp-snooping timeout 查看是否设置成功。

第 8 章 配置链路捆绑 Trunking

Trunking功能可以把多个物理端口捆绑起来当作一个逻辑端口来使用，这样做能够增加带宽、提供冗余度和流量的均衡。捆绑起来的逻辑链路根据所配置的选择规则在各个物理链路上动态分配发送的数据流量。参与捆绑物理端口应在同一个VLAN内。

8.1 选择准则

交换机根据端口选择准则决定数据发送到哪个物理端口。端口选择准则有以下几种：

- ✧ smac 基于源MAC地址
- ✧ dmac 基于目的MAC地址
- ✧ sdmac 基于源和目的MAC地址异或的值
- ✧ sip 基于源ip地址
- ✧ dip 基于目的ip地址
- ✧ sdip 基于源和目的ip地址异或的值

 系统缺省为 smac。

注意：

系统只有在发送数据时才参考选择准则，实现数据流量的均衡。

8.2 配置Trunking

创建逻辑捆绑链路

【命令1】 channel-group add *linknum portlist criterion*

〖参数说明〗逻辑链路号“linknum”的取值范围是1-24;

“portlist” 是组端口成员（格式为 xxmxxm.其中xx是实际物理端口号）;

“criterion”选择标准，其值是smac,dmac,sdmac,sip,dip,sdip之一。

〖命令模式〗配置模式

〖参考举例〗 switch(config)# channel-group add 2 02m05m sdmac

上述操作将配置组号为 2 的 trunk 组，其成员端口为 2 和 5 端口，发送数据时选择规则为 sdmac 方式，即用源 mac 地址与目的 mac 地址异或值做为端口选择的参考值。

注意：注意成员端口必须属于同一个 VLAN.

删除逻辑捆绑链路

【命令1】 channel-group delete *linknum*

〖参数说明〗逻辑链路号“linknum”的取值范围是1-24;
〖命令模式〗配置模式
〖参考举例〗switch(config)# channel-group delete 2
上述操作将删除组号为 2 的 trunk 组。

全局模式下键入 show channel-group 查看是否设置成功，即：
switch#show channel-group 。

第 9 章 配置访问控制列表（ACL）

本交换机的所有访问控制列表 ACL 是针对实际物理端口设置的，因此访问控制列表里所配置的端口列表成员无须受其他配置的约束（例如，端口列表的成员可以在不同的 VLAN 内）。本交换机提供了丰富灵活的访问控制列表配置规则，可以在单条访问控制列表内一次设置很多过滤选项（包括源或目的 MAC 地址、虚拟局域网号 VLAN_ID、源或目的 IP 地址、协议类型及源或目的协议端口号（对于 TCP/UDP 协议来说方可配置，其他协议不能配置）、IP 优先级（IP_Precedence 字段）或 DIFFSERV（IP_Diffserv 字段，其对 TOS 字段（共八位）重新定义，只使用前六位，后两位为保留位））等，也可在单条访问控制列表内只设置单个过滤选项。

另外，每条访问控制列表必须设置各自的优先级。**若在同一个端口列表上有多条配置了不同优先级的访问控制列表同时使能启用，则进入交换机的数据报将严格按照优先级从高到低的顺序依次匹配所有已经使能启用的访问控制列表，若其同时符合多条规则，则将按照优先级最高的访问控制列表来处理；若只符合其中一条规则，则将按照此条访问控制列表进行处理；若对于所有已启用的访问控制列表都不符合，则按照指定的缺省动作来进行相应的处理。**

注意：**缺省动作可以通过配置命令在各个端口列表上单独指定。在配置缺省动作前，必须已经配置了与其具有相同端口列表的访问控制列表，否则无法进行配置。**在所有的端口列表上默认的缺省动作都是“permit”，即允许任何不符合所有已启用的访问控制列表的数据报都通过；用户可以使用配置命令来指定在相应端口列表上的缺省动作为“deny”，即禁止任何不符合所有已启用的访问控制列表的数据报通过。另外，**在配置各条访问控制列表时，必须保证其相应的端口列表不可重叠，否则不允许配置。**例如：端口列表<01m02m03m04m>和<03m04m05m06m> 便在物理端口 03、04 上产生了重叠。

在配置交换机的访问控制列表时，需要首先定义访问控制列表，再启用这些访问控制列表使其生效。

9.1 定义访问控制列表规则

可基于源或目的 MAC 地址、虚拟局域网号 VLAN_ID、源或目的 IP 地址、协议类型、源或目的协议端口号（对于 TCP/UDP 协议来说方可配置，其他协议不能配置）、IP 优先级（IP_Precedence 字段）或 DIFFSERV 等过滤选项来定义相应的访问控制列表，同时在配置命令中必须设定每条访问控制列表的优先级。**注意：在配置各条访问控制列表时，对于具有相同过滤选项和相同动作（允许或禁止）的访问控制列表，应使他们具有相同的优先级；不同过滤选项或不同动作的各条访问控制列表，则都应使其具有不同的优先级。**为了便于说明如何定义访问控制列表，这里先说明只根据单个过滤选项来定义的单项访问控制列表，再说明根据多个过滤选项来定义的复合访问控制列表。复合访问控制列表只是由多个过滤选项来构成，而单项访问控制列表只有一个过滤选项，别无区别。在复合访问控制列表中，只有符合了所有过滤选项条件的数据报才会按照此复合访问控制列表所定义的动作（“permit”或“deny”）进行转发或者丢弃。

9.1.1 定义访问控制列表的全局参数

【命令 1】access-list ruleid *ruleid* <deny | permit> priority *priority* <*portlist* | default>

〖命令说明〗定义并进入一条访问控制列表的配置模式

〖参数说明〗

- ✧ “ruleid”：列表序号，取值范围是0 – 999 ；
- ✧ <deny|permit> ：设置允许还是拒绝符合规则的数据报通过 。
- ✧ “priority”：此条规则所要设定的优先级，取值范围是0-7。
- ✧ “portlist”：表示参与该访问控制列表的端口成员，以下方式输入：
  端口号+m
  例如02m15m，表示2端口和15端口为此条访问控制列表在其上生效的物理端口，注意上述命令的02 不要写成 2 。
- ✧ “default” ：在所有物理端口上都使用此条访问控制列表 。

〖命令模式〗配置模式

〖参考举例〗

```
switch(config)# access-list ruleid 2 deny priority 2 08m13m
```

上述操作设置一条访问控制列表，过滤列表序号是 2，优先级是 2 ，在端口 8 和 13 上将禁止符合此条访问控制列表的数据报通过。

☞ 在全局模式下，用 show access-list ruleid *ruleid* 查看是否设置成功。

9.1.2 定义基于MAC地址的过滤选项

【命令 1】subset mac <*aa:aa:aa:aa:aa:aa* | any> <*bb:bb:bb:b:bb:bb* | any>

〖命令说明〗定义基于源和目的 mac 地址的过滤选项的访问控制列表

〖参数说明〗

- ✧ “ aa:aa:aa:aa:aa:aa” ： 将 被 过 滤 的 目 的 mac 地 址 ， 如 ： 00:34:3d:22:00:45 ，若不需要过滤目的mac地址，则设置为“any”即可。
- ✧ “ bb:bb:bb:bb:bb:bb” ： 将 被 过 滤 的 源 mac 地 址 ， 如 ： 00:05:5d:67:66:ca ，若不需要过滤源mac地址，则设置为“any”即可。

〖命令模式〗访问控制列表的配置模式

〖参考举例〗

```
switch(config-acl)# subset mac any 00:4d:23:45:4e:0a
```

上述操作设置一条访问控制列表的 mac 地址过滤选项为：目的 mac 地址不限，源 mac 为 00:4d:23:45:4e:0a 。

☞ 在全局模式下，用 show access-list ruleid *ruleid* 可查看此过滤选项是否设置成功。

9.1.3 定义基于VLAN_ID的过滤选项

【命令 1】subset vlan-id *vlan-id*

〖命令说明〗定义基于 vlan-id 的过滤选项的访问控制列表

〖参数说明〗

✧ “vlan-id”：将被过滤的VLAN_ID值，取值范围是1 – 4094 。

〖命令模式〗访问控制列表的配置模式

〖参考举例〗

```
switch(config-acl)# subset vlan-id 12
```

上述操作设置一条访问控制列表的 vlan-id 过滤选项为 12 。

☞ 在全局模式下，用 show access-list ruleid *ruleid* 可查看是否设置成功。

9.1.4 定义基于IP优先级（IP_Precedence）的过滤选项

【命令 1】subset precedence <match | set> *precedence*

〖命令说明〗定义基于 ip_precedence 的过滤选项的访问控制列表

〖参数说明〗

✧ “match”：设置匹配“*precedence*”值的数据报才符合此条访问控制列表。

✧ “set” ：符合此条访问控制列表的数据报的 ip_precedence 字段将被设置为“*precedence*”值。

✧ “precedence”：将被匹配或设置的 ip_precedence 值，取值范围是0 – 7 。

〖命令模式〗访问控制列表的配置模式

〖参考举例〗

```
switch(config-acl)# subset precedence match 3
```

上述操作设置进入相应物理端口列表的数据报，其 ip_precedence 值等于 3 才符合此条访问控制列表 。

☞ 在全局模式下，用 show access-list ruleid *ruleid* 可查看是否设置成功。

9.1.5 定义基于DIFFSERV（IP_Diffserv）的过滤选项

【命令 1】subset diffserv <match | set> *diffserv*

〖命令说明〗定义基于 ip_diffserv 的过滤选项的访问控制列表

〖参数说明〗

✧ “match”：设置匹配“*diffserv*”值的数据报才符合此条访问控制列表。

✧ “set” ：符合此条访问控制列表的数据报的 ip_diffserv 字段将被设置为“*diffserv*”值。

✧ “diffserv”：将被匹配或设置的 ip_diffserv 值，取值范围是0 – 63 。

〖命令模式〗访问控制列表的配置模式

〖参考举例〗

```
switch(config-acl)# subset diffserv match 25
```

上述操作设置进入相应物理端口列表的数据报，其 ip_diffserv 值等于 25 才符合此条访问控制列表 。

☞ 在全局模式下，用 show access-list ruleid *ruleid* 可查看是否设置成功。

9.1.6 定义基于IP地址的过滤选项

【命令 1】 subset ip <*a. b. c. d x. x. x. x* | any> <*e. f. g. h x. x. x. x* | any>

〖命令说明〗在访问控制列表中定义基于源和目的 ip 地址的过滤选项

〖参数说明〗

- “a. b. c. d”：将被过滤的源ip地址，如：192.168.1.98，随后的“x. x. x. x”为其掩码；当不需要过滤源ip地址时，则设置为“any”即可。注意：当用户希望过滤某一网段内的数据报时，则这时的“a. b. c. d”必须设置为相应的网络值，掩码也是网络值；当用户希望过滤某一主机的数据报时，则这时的“a. b. c. d”必须设置为相应的主机ip地址，掩码应为“255.255.255.255”。
- “e. f. g. h”：将被过滤的目的ip地址，如：192.168.2.100，随后的“x. x. x. x”为其掩码；当不需要过滤源ip地址时，则设置为“any”即可。注意：当用户希望过滤某一网段内的数据报时，则这时的“e. f. g. h”必须设置为相应的网络值，掩码也是网络值；当用户希望过滤某一主机的数据报时，则这时的“e. f. g. h”必须设置为相应的主机ip地址，掩码应为“255.255.255.255”。

〖命令模式〗访问控制列表的配置模式

〖参考举例〗

```
switch(config-acl)# subset ip any 192.168.1.0 255.255.255.0
```

上述操作设置一条访问控制列表的 ip 地址过滤选项为：源 ip 地址不限，目的 ip 地址为 192.168.1.0 网段内 。

☞ 在全局模式下，用 show access-list ruleid *ruleid* 查看是否设置成功。

注意：所配置的ip地址与子网掩码必须是对应的，若针对某个指定的主机 IP 地址如 192.168.1.98 定义访问控制列表，则掩码必须是 255.255.255.255 ，而不是255.255.255.0 ；若针对某个网段地址如 192.168.1.0 定义访问控制列表，则掩码必须是255.255.255.0 。

9.1.7 定义基于PROTOCOL协议类型的过滤选项

【命令 1】 subset protocol *protocol*

〖命令说明〗定义一条基于协议的访问控制列表

〖参数说明〗

- “protocol”：将被过滤的协议类型，取值范围是<1-255> ，例如：icmp 为 1 ，igmp 为 2 ，tcp 为 6 ，udp 为 17，ospf 为 89 ，也可以直接输入几个常用的协议名称，例如icmp，igmp，tcp，udp 等。对于tcp和udp报文来说还可以输入源或目的协议端口号，对于tcp报文来说还可以通过此项命令直接实现单向访问（对于tcp协议来说，在建立连接阶段会向对方发送连接请求，从而可以直接达到实现单向访问的目的，对于udp来说，

可以通过源/目的协议端口号来实现单向访问的目的），下面将举例说明。

〖命令模式〗访问控制列表的配置模式

〖参考举例〗

switch(config-acl)# subset protocol 1

上述操作在某条访问控制列表中设置一个针对 icmp 协议的过滤选项。

switch(config-acl)# subset protocol tcp established dst-port 21

上述操作在某条访问控制列表中设置一个针对 tcp 协议，且其目的端口为 21 的 tcp 协议连接请求进行控制的过滤选项。

switch(config-acl)# subset protocol udp dst-port 69

上述操作在某条访问控制列表中设置一个针对 udp 协议，且其目的端口为 69 的数据流进行控制的过滤选项，69 为 tftp 协议的服务端口。

☞ 在全局模式下，用 show access-list ruleid *ruleid* 查看是否设置成功。

9.1.8 定义在某个端口列表上的缺省动作

【命令 1】access-list default set *portlist* <deny | permit>

〖命令说明〗定义在某个端口列表上的缺省动作

〖参数说明〗

✧ “portlist”：表示参与该访问控制列表的端口成员，以下方式输入 ：

端口号+m

例如02m15m，表示2端口和15端口为此条访问控制列表在其上生效的物理端口，注意上述命令的02 不要写成 2 。

✧ <deny|permit> ：允许还是拒绝通过的选项,默认是“permit”。

〖命令模式〗配置模式

〖参考举例〗

switch(config)# access-list default set 08m13m deny

上述操作在物理端口 08，13 上设置了缺省动作“deny”，即在物理端口 08，13 上不符合任何已启用的访问控制列表的数据报都将被丢弃。

☞ 在全局模式下，用 show access-list default 即可查看所有访问控制列表的端口列表上的缺省动作。

注意：在配置在某个端口列表上的缺省动作时，应已经配置了至少一条具有相同端口列表的访问控制列表，否则无法配置，因为在这种情况下的配置是没有意义的。默认情况下，对于所有的端口列表来说，其缺省的动作都是“permit”，即允许任何不符合所有已启用的访问控制列表的数据报都通过 。

9.2 定义复合访问控制列表

复合访问控制列表即为基于两个或两个以上过滤选项来定义的访问控制列表。过滤选项包括源或目的 MAC 地址，虚拟局域网号 VLAN_ID，源或目的 IP 地址，协议类型及源

或目的端口号，IP 优先级（IP_Precedence）或 DIFFSERV（IP_Diffserv）等，它们可以任意组合以形成较为复杂的复合访问控制列表以控制一些特殊的数据流。复合访问控制列表所使用的访问控制选项越多，则对进入相应端口列表的数据报的过滤限制越严格。由于复合访问控制列表比单项访问控制列表仅仅多了一些过滤选项，配置也比较简单，这里就不再举例说明，在使用时可以举一反三，依此类推。

9.3 删除访问控制列表或其过滤选项

虽然各种基于源或目的 MAC 地址，虚拟局域网号 VLAN_ID，源或目的 IP 地址，协议类型及源或目的端口号，IP 优先级（IP_Precedence）或 DIFFSERV（IP_Diffserv）的访问控制列表的配置命令不同，但是删除这些访问控制列表的命令却是相同的，下面详细说明。注意：在删除访问控制列表或其过滤选项时，应保证此访问控制列表没有启用。

9.3.1 删除访问控制列表的过滤选项

【命令 1】 no subset <mac | vlan-id | ip | protocol | precedence | diffserv>

〖命令说明〗删除访问控制列表的某个过滤选项

〖参数说明〗

- ✧ “mac”：基于 mac 地址的过滤选项。
- ✧ “vlan-id”：基于 vlan-id 地址的过滤选项。
- ✧ “ip”：基于 ip 地址的过滤选项。
- ✧ “protocol”：基于 protocol 协议类型的过滤选项。
- ✧ “precedence”：基于 ip_precedence 的过滤选项。
- ✧ “diffserv”：基于 ip_diffserv 的过滤选项。

〖命令模式〗访问控制列表的配置模式

〖参考举例〗

```
switch(config-acl)# no subset precedence
```

上述操作删除某条访问控制列表中的 precedence 过滤选项 。

9.3.2 删除整条访问控制列表

【命令 1】 no access-list ruleid *ruleid*

〖命令说明〗删除一条访问控制列表

〖参数说明〗“ruleid”是列表序号，取值范围是0-999 ；

〖命令模式〗配置模式

〖参考举例〗

```
switch(config)# no access-list ruleid 2
```

上述操作删除访问控制列表 2 。

注意：在删除访问控制列表或其过滤选项时，应保证此访问控制列表没有启用，否则将给予相应的提示信息。

9.4 使访问控制列表生效或失效

使这些访问控制列表生效或失效的命令非常简单，下面详细说明。

9.4.1 使访问控制列表生效或失效

【命令 1】packet-filter enable ruleid *ruleid*

〖命令说明〗使一条访问控制列表生效

〖参数说明〗“ruleid” 是在access-list中定义的列表序号，取值范围是0-999 ；

〖命令模式〗配置模式

〖参考举例〗

```
switch(config)# packet-filter enable ruleid 2
```

上述操作使访问控制列表 2 生效 。

【命令 2】packet-filter disable ruleid *ruleid*

〖命令说明〗使一条访问控制列表失效

〖参数说明〗“ruleid” 是在access-list中定义的列表序号，取值范围是0-999 .

〖命令模式〗配置模式

〖参考举例〗

```
switch(config)# packet-filter disable ruleid 2
```

上述操作使访问控制列表 2 失效。

注意：各种访问控制列表在定义后默认是不生效的，必须手动配置使访问控制列表生效的命令才能启用相应的访问控制列表;若某条访问控制列表的当前状态是不生效的，则配置使其失效的命令将不起任何作用。

第 10 章 端口镜像(mirroring)

端口镜像是指通过将一个或多个端口的数据复制到指定的交换机端口上,从而可进行网络流量分析和错误诊断等。

10.1 镜像规则分类

根据数据的流的方向分:

- ✧ 输入数据镜像
- ✧ 输出数据镜像
- ✧ 根据数据流类型镜像

交换机支持以上规则的混合。

10.2 配置基于端口的镜像规则

10.2.1 配置参与镜像的源端口

镜像源端口是参与镜像的源端口,即它上面的数据将被系统复制一份发给镜像的目的端口。配置镜像源端口,利用命令:

【命令 1】mirror link-group set *link-group portnum <egress/ingress/both>*

〖命令说明〗指定一个端口为镜像源端口,并指定是对该端口的输入数据还是输出数据镜像。

〖参数说明〗"*link-group*"是镜像端口组的索引号,范围是1-24;"portnum"是端口号+m,取值范围是1-24,egress表示只对输出数据镜像,ingress表示只对输入数据镜像,both表示对输入输出数据镜像。

〖命令模式〗配置模式

〖参考举例〗switch(config)# mirror link-group set 1 02m ingress

上述命令指定流量镜象的源端口,本例中是将端口 2 指定为源端口,并且只镜象其上的输入流量。


可以用上述命令指定多个源端口

10.2.2 配置镜像目标端口

镜像目标端口,指数据复制到的目标端口。任何一个交换机带内端口都可以作为一个目标端口。指定镜像的目标端口,利用命令:

【命令 1】mirror mirrored-to *portnum*

〖命令说明〗指定一个端口为镜像目标端口

〖参数说明〗"portnum" 是端口号,取值范围是1-24。

〖命令模式〗配置模式

〖参考举例〗switch(config)# *mirroring to 10*

上述命令指定流量镜象的目的端口,该例是端口 10。

该目标端口是所有的指定的源端口目标端口

10.2.3 使基于端口的镜像镜像规则生效或失效

【命令 1】mirror link-group <*enable/disable*> *link-group*

〖命令说明〗使镜像生效或失效

〖参数说明〗“*enable*”,表示使镜像生效,“*disable*”,表示使镜像失效,“*link-group*”是镜像端口组的索引号，范围是1-24，该索引号必须是已经定义好的镜像规则。

〖命令模式〗配置模式

〖参考举例〗switch(config)# mirror link-group enable 1

上述命令使镜象组 1 生效

在全局模式下，可以用 show mirr all 查看镜象配置情况。

10.2.4 删除基于端口的镜像规则

用下面的命令删除镜像规则。

【命令 1】no mirror link-group <*link-group*>

〖命令说明〗删除镜像规则

〖参数说明〗“*link-group*”是镜像端口组的索引号，范围是1-24，该索引号必须是已经定义好的镜像规则。

〖命令模式〗配置模式

〖参考举例〗switch(config)# no mirr link-group 1

上述命令镜象组 1 删除。即源端口 2 上的输入流量不再镜象到目的端口。



删除镜像规则时，只是删除镜像源端口即可，无须删除镜像目的端口。

10.3 配置基于访问控制列表的镜像规则

10.3.1 配置参与镜像的访问控制列表

建立访问控制列表与镜像规则之间的关联,符合这种规则的数据将被系统复制一份发给镜像的目的端口。

【命令 1】mirror acl-group set <*acl-group*> access-list ruleid <*ruleID*>

〖命令说明〗指定参与镜像的访问控制列表

〖参数说明〗“*acl-group*”是镜像访问列表组的索引号，范围是0-999；“*ruleID*”是访问列表的序列号，该访问控制列表必须是已经存在的。

〖命令模式〗配置模式

〖参考举例〗switch(config)# mirror acl-group set 1 access-list ruleid 1

上述命令指定符合访问控制列表 1 的流量将被系统复制并且镜像到镜像目的端口。

10.3.2 配置镜像目标端口

镜像目标端口，指数据复制到的目标端口。任何一个交换机带内端口都可以作为一个目标端口。指定镜像的目标端口，利用命令：

【命令 1】mirror mirrored-to *portnum*

〖命令说明〗指定一个端口为镜像目标端口

〖参数说明〗“portnum” 是端口号，取值范围是1-24。

〖命令模式〗配置模式

〖参考举例〗switch(config)# *mirroring to 10*

上述命令指定流量镜象的目的端口，该例是端口 10。

☞ 该目标端口是所有的指定的源端口目标端口

10.3.3 使基于访问控制列表的镜像镜像规则生效或失效

【命令 1】mirror acl-group <*enable*/*disable*> *acl-group*

〖命令说明〗使镜像生效或失效

〖参数说明〗“*enable*”，表示使镜像生效，“*disable*”，表示使镜像失效，“*acl-group*”是镜像端口组的索引号，范围是0-999，该索引号必须是已经定义好的镜像规则。

〖命令模式〗配置模式

〖参考举例〗switch(config)# mirror acl-group enable 1

上述命令使镜象组 1 生效

 在全局模式下，可以用 show mirror all 查看镜象配置情况。

10.3.4 删除基于访问控制列表的镜像规则

用下面的命令删除镜像规则。

【命令 1】no mirror acl-group <*acl-group*>

〖命令说明〗删除镜像规则

〖参数说明〗“*acl-group*”是镜像端口组的索引号，范围是0-999，该索引号必须是已经定义好的镜像规则。

〖命令模式〗配置模式

〖参考举例〗switch(config)# no mirror acl-group 1

上述命令镜象组 1 删除。即符合该镜像规则相关联的访问控制列表的流量不再镜象到目的端口。

 删除镜像规则时，只是删除镜像源端口即可，无须删除镜像目的端口。

第 11 章 Quality of Service(QoS)

本交换机支持 801.1p 协议，已经实现了基于端口的优先级映射，基于 ACL 流的优先级映射，基于 DIFFSERV 的优先级映射（配置方式类似于基于 ACL 流的优先级映射，通过在 ACL 中配置过滤选项 DIFFSERV 值来实现，下面不再赘述），基于 TOS（TOS_Precedence）的优先级映射等多种映射策略，并且提供了严格队列模式和加权队列模式两种队列调度模式，可以根据配置为数据流加上相应优先级标记，并有 8 个优先级队列，充分保证关键数据流带宽，最大限度降低时延，从而保证网络服务质量，有效支持语音视频等实时关键业务。

QoS 配置主要分 5 部分：

✧ 设置 QOS 队列调度模式

✧ 设置基于端口的优先级映射

✧ 基于 ACL 流的优先级映射

✧ 基于 TOS 的优先级映射

11.1 优先级映射规则说明

当含有 VLAN_TAG 标记的以太网帧进入端口到达交换机内时，系统按照设定的规则，根据 TAG 域内的 802.1p 优先级自动将该数据帧放到相应的硬件优先级发送队列中，硬件队列的优先级有 8 个(取值范围: 0 – 7)，其与 802.1p 映射关系如表 11-1 所示。需要说明的是，在这里 802.1p 优先级是按照从小到大依次增大的，即 0 是最低优先级，7 是最高优先级，同硬件发送队列的优先级完全相同。无论处于严格队列模式下，还是处于加权队列模式下，当接收端口处于过载状态时，越高优先级的数据流的时延（Latency）越低 ，在接收端口处于过载状态时的丢包率（Loss）也越少或不丢包（视过载程度而定）；反之，越低优先级的数据流的时延越高，丢包率也越大。在没有启用 QOS 模块时，所有数据流的优先级都默认为 0 ，即对于不同优先级的数据流都将平等对待，当接收端口处于过载状态时，则无论其优先级大小，丢包率都相同，时延也相同。

表11-1 802.1p 与硬件队列映射关系

802.1p优先级	硬件队列优先级
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

11.2 设置QOS队列调度模式

QOS 共有两种队列调度模式：严格队列模式和加权队列模式。两者的区别在于：当多个具有不同优先级的数据流同时到达某个端口，并且导致此端口处于过载状态时，在使用严格队列模式的情况下，系统将会把超过满负荷的最低优先级的过载数据流首先丢弃，直到端口恰好处于满负荷状态；而在使用加权队列模式的情况下，系统将会根据数据流的优先级大小，把超过满负荷的的过载数据流也优先级的大小按比例丢弃，即优先级越低的数据流丢包率越多，优先级越高的数据流丢包率越少或不丢包（视过载程度而定），直到端口恰好处于满负荷状态 。举例说明如下：假如有优先级从 0 到 7 的 8 个不同优先级的数据流同时到达某个端口，假如它们发包的速率都为 此端口接收数据包能力的30% ，那末所有数据流的发包率之和为 30% × 8 ＝ 240% ，显然，此端口将会处于过载状态 。如果设置 QOS 处于严格队列模式，这时优先级为 5，6，7 的数据流全部被转发，优先级为 4 的数据流有 1/3 被转发，其余部分全部丢弃；优先级为 0，1，2，3 的数据流全部丢弃；如果设置 QOS 处于加权队列模式，这时将会优先级为 7 的数据流的丢包率最小或者不丢包，优先级为 7 的数据流的丢包率稍微多一些，依次递增，优先级为 0 的数据流的丢包率最大的情况。

设定 QOS 硬件队列调度模式

【命令 1】traffic-policy running-mode strict-queue

〖命令说明〗设定 QOS 调度模式为严格队列模式

〖参数说明〗

〖命令模式〗配置模式

〖参考举例〗

【命令 2】traffic-policy running-mode weighted-queue

〖命令说明〗设定 QOS 调度模式为加权队列模式

〖参数说明〗

〖命令模式〗配置模式

〖参考举例〗

 即使优先级映射策略已经被启用，也可以随时设定或更改 QOS 的调度模式。

11.3 设置基于端口的优先级映射

基于端口的优先级映射，是针对于那些进入交换机之前不带 VLAN_TAG 标记的数据流，系统将会根据下面配置的优先级把这些数据流分别映射到相应的硬件发送队列。

【命令 1】traffic-policy link-group set <1-24> <portlist> local-precedence <0-7>

〖命令说明〗设置对不带 VLAN_TAG 标记的数据流的优先级映射规则

〖参数说明〗

- ✧ “<1-24>”：映射规则的序号。
- ✧ “<portlist>”：表示参与该映射规则的端口成员，以下方式输入：

端口号+m

例如02m12m，表示2端口和12端口为这个映射规则的端口成员，注意

上述命令的02 不要写成 2 。

- ✧ “<0-7>”：此条映射规则对规则内的端口成员所要设定的优先级。

〖命令模式〗配置模式

〖参考举例〗

switch(config)# traffic-policy link-group set 1 01m02m local-precedence 7

上述操作设定一条针对端口成员 01m02m 的优先级映射规则，映射规则序号是 1，优先级是 7 ，该映射规则将设定从端口 1 和 2 进入的数据流的优先级为 7，这些数据流将会被放入接收端口的硬件发送队列 7 中。

☞ 在全局模式下，用 **show traffic-policy link-group <1-24>** 可查看是否设置成功及相关信息:

```
switch# show traffic-policy link-group 1
traffic-policy running-mode: weighted-queue

traffic-policy link-group  1
current state: inactive
portlist: 01m02m
```

【命令 2】traffic-policy link-group enable <1-24>

〖命令说明〗启用一条基于端口的优先级映射规则

〖参数说明〗

- ✧ “<1-24>”：映射规则的序号。

〖命令模式〗配置模式

〖参考举例〗

switch(config)# traffic-policy link-group enable 1

上述操作启用一条序号为 1 的基于端口的优先级映射规则。

☞ 在全局模式下，用 **show traffic-policy link-group <1-24>** 可查看此映射规则是否处于启用状态。

注意：上述配置只对进入映射规则所设定的成员端口，且不带VLAN_TAG标记的数据流有效。

【命令 3】traffic-policy link-group disable <1-24>

〖命令说明〗禁用一条基于端口的优先级映射规则

〖参数说明〗

- ✧ “<1-24>”：映射规则的序号。

〖命令模式〗配置模式

〖参考举例〗

switch(config)# traffic-policy link-group enable 1

上述操作禁用一条序号为 1 的基于端口的优先级映射规则。

☞ 在全局模式下，用 **show traffic-policy link-group <1-26>**可查看此映射

规则是否处于禁用状态。

【命令 4】no traffic-policy link-group <1-24>

〖命令说明〗删除一条基于端口的优先级映射规则

〖参数说明〗

✧ “<1-24>”：映射规则的序号。

〖命令模式〗配置模式

〖参考举例〗

```
switch(config)# no traffic-policy link-group 1
```

上述操作删除一条序号为 1 的基于端口的优先级映射规则。

☞ 在全局模式下，用 show traffic-policy link-group <1-24>可查看此映射规则是否已被删除。

11.4 基于ACL流的优先级映射

基于 ACL 流的优先级映射，是针对于那些符合特定 ACL 规则的数据流，系统将会根据下面配置的优先级规则，把这些数据流分别映射到相应的硬件发送队列。需要说明的是，在启用基于 ACL 流的优先级映射规则之前，必须保证相应的 ACL 规则处于启用状态，并且这些 ACL 规则应为“permit”模式（若这些 ACL 规则为“deny”模式，则符合这些 ACL 规则的数据流将被 ACL 规则丢弃，故不会被映射到硬件发送队列中）。ACL 规则的配置及启用请参见“配置访问控制列表”的相应章节，这里不再赘述。

【命令 1】traffic-policy acl-group set <0-999> access-list ruleid <0-999> local-precedence <0-7>

〖命令说明〗设置一条基于 ACL 流的优先级映射规则

〖参数说明〗

✧ “<0-999>”：映射规则的序号。

✧ “<0-999>”：访问控制列表access-list（简称 ACL）的序号。

✧ “<0-7>”：此条映射规则对某条访问控制列表所要设定的优先级。

〖命令模式〗配置模式

〖参考举例〗

```
switch(config)# traffic-policy acl-group set 1 access-list
        ruleid 1 local 7
```

上述操作设定一条针对访问控制列表 1 的优先级映射规则，映射规则的序号是 1，优先级是 7，该映射规则将设定符合访问控制列表 1 的数据流的优先级为 7，这些数据流将会被放入接收端口的硬件发送队列 7 中。

☞ 在全局模式下，用 show traffic-policy acl-group <0-999> 可查看是否设置成功及相关信息:

```
switch# show traffic-policy acl-group 1
traffic-policy running-mode: weighted-queue

traffic-policy acl-group  1
```

```
current state: inactive
refer to access-list ruleid: 1
```

【命令 2】traffic-policy acl-group enable <0-999>

〖命令说明〗启用一条基于 ACL 流的优先级映射规则

〖参数说明〗

✧ "<0-999>"：映射规则的序号。

〖命令模式〗配置模式

〖参考举例〗

```
switch(config)# traffic-policy acl-group enable 1
```

上述操作启用一条序号为 1 的基于 ACL 流的优先级映射规则。

☞ 在全局模式下，用 show traffic-policy acl-group <0-999> 可查看此映射规则是否处于启用状态。

【命令 3】traffic-policy acl-group disable <0-999>

〖命令说明〗禁用一条基于 ACL 流的优先级映射规则

〖参数说明〗

✧ "<0-999>"：映射规则的序号。

〖命令模式〗配置模式

〖参考举例〗

```
switch(config)# traffic-policy acl-group enable 1
```

上述操作禁用一条序号为 1 的基于 ACL 流的优先级映射规则。

☞ 在全局模式下，用 show traffic-policy acl-group <0-999>可查看此映射规则是否处于禁用状态。

【命令 4】no traffic-policy acl-group <0-999>

〖命令说明〗删除一条基于 ACL 流的优先级映射规则

〖参数说明〗

✧ "<0-999>"：映射规则的序号。

〖命令模式〗配置模式

〖参考举例〗

```
switch(config)# no traffic-policy acl-group 1
```

上述操作删除一条序号为 1 的基于 ACL 流的优先级映射规则。

☞ 在全局模式下，用 show traffic-policy acl-group <0-999>可查看此映射规则是否已被删除。

11.5 基于TOS的优先级映射

基于 TOS（TOS_Precedence）的优先级映射，是针对于数据包中 IP 头部内 TOS（Type of Service，总共 8 bit）的 precedence 字段值（前 3 bit）而设定，系统将会根据下面配置的优先级规则，把这些数据流分别映射到相应的硬件发送队列。需要说明的是，

precedence 总共有 3 bit，故有 8 个优先级值（取值范围：0 – 7），它和硬件发送队列的对应关系如表 11-2。有些交换机也有设置 TOS 字段值或根据 TOS 字段值来做一些特殊处理的选项，但是它的含义和本交换机不一定是相同的，一定要注意仔细区分。比如，cisco3550 三层交换机的 TOS 是指 IP 头部内 TOS 的后 4 bit ，即服务类型（Type of service）字段值，它总共有 4 bit ，故有 16 个优先级值(取值范围：0 – 15)。

表11-2　TOS优先级硬件队列映射关系

TOS优先级	硬件队列优先级
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

【命令 1】traffic-policy tos set default <*portlist*>

〖命令说明〗设置基于 TOS 的优先级映射规则

〖参数说明〗“<portlist>”：表示参与该映射规则的端口成员，以下方式输入：

端口号+m

例如02m12m，表示2端口和12端口为这个映射规则的端口成员，注意上述命令的02 不要写成 2 。此参数也可以不设置，即对所有端口都启用。

〖命令模式〗配置模式

〖参考举例〗

 在全局模式下，用 show traffic-policy tos 可查看是否设置成功及相关信息：

```
switch# show traffic-policy tos
traffic-policy running-mode: weighted-queue

traffic-policy tos class
current state: inactive
local-precedence: default
relative portlist: all the ports
```

【命令 2】traffic-policy tos enable

〖命令说明〗启用基于 TOS 的优先级映射规则

〖参数说明〗

〖命令模式〗配置模式

〖参考举例〗

在全局模式下，用 show traffic-policy tos 可查看此映射规则是否处于启用状态。

【命令 3】traffic-policy tos disable

〖命令说明〗禁用基于 TOS 的优先级映射规则

〖参数说明〗

〖命令模式〗配置模式

〖参考举例〗


在全局模式下，用 show traffic-policy tos 可查看此映射规则是否处于禁用状态。

【命令 4】no traffic-policy tos

〖命令说明〗删除基于 TOS 的优先级映射规则

〖参数说明〗

〖命令模式〗配置模式

〖参考举例〗


在全局模式下，用 show traffic-policy tos 可查看此映射规则是否已被删除。

第 12 章 配置虚拟接口

虚拟接口是指是以一个 VLAN 作为一个接口，为其配置 IP 地址，该接口对外如同路由器的一个实际物理接口一样。虚拟接口上可以配置多个子网接口，每个子网接口对应不同 IP 地址，每个子接口独立工作。但他们都通过相同的 VLAN 来收发数据包。 注意这个虚拟接口不是与交换机实际的物理端口对应的，而是与 VLAN 对应。

12.1 配置子网接口

配置子网接口，首先要按**第 4 章 “配置 VLAN”**，设置 VLAN。只有成功设置 VLAN 后，再进行下面的配置。

增加 IP 子网接口

【命令 1】 ip address add vint *vintnum ipaddr netmask* vid *vidnum* description *string*

〖命令说明〗增加一个子网接口

〖参数说明〗“vintnum”是虚拟子网接口序号，取值范围是0-31；
“ipaddr” 是该子网接口的IP地址，类型是A.B.C.D,注意此地址不能与其他任何接口地址相同；
“netmask” 是子网掩码；
“vidnum” 是为该虚拟接口对应的VLAN序号；
“string” 表示对该虚拟接口的描述文字，用于标识记忆。

〖命令模式〗配置模式

〖参考举例〗switch(config)# ip address add vint 2 2.2.2.2 255.255.255.0 vid 3 description testing

上述命令把 VLAN 3 指定为子接口 2（vint 2），为这个接口配了 2.2.2.2 的 IP 地址，掩码是 255.255.255.0,接口描述为 testing。

☞ 在全局模式下，上述配置可以用 show ip address 查看是否配置成功， 若成功应显示含有下面信息：

Row	Vint	Ip Address	Subnet Mask	VID	Description	Status
2	2	2.2.2.2	255.255.255.0	3	testing	active

注意：

指定的对应 VLAN 应该是存在的,所配的地址不能与其他任何接口地址相同。

删除 IP 子网接口

【命令 3】 ip address delete ipaddr

〖命令说明〗删除一个子网接口

〖参数说明〗“ipaddr” 是该子网接口的IP地址，类型是A.B.C.D,注意此地址不能与其他任何接口地址相同；

〖命令模式〗配置模式

〖参考举例〗switch(config)# ip address delete 2.2.2.2

上述命令把地址为 2.2.2.2 的子网删除。

注意：该配置并不删除子网接口对应的VLAN。

WEB CONFIG 12.1-1

IP 子网

IP 子网配置						
子网	Vlnt	IP 地址	子网掩码	VID	描述	状态
new		0.0.0.0		0		
1	Vlnt1	3.3.3.3	255.255.255.0	2	--None--	active
2	Vlnt2	4.4.4.4	255.255.255.0	3	--None--	active

第 13 章 配置路由

三层交换机不但具备二层交换功能，而且具备三层路由功能，三层路由功能是三层交换机区别于二层交换机的重要概念。三层交换机本身具备路由协议，负责路由的建立，实现不同子网的数据转发。

本章包括如下内容：

✧ 静态路由配置指导

✧ RIP V1/V2协议配置指导

✧ OSPF Version 2协议配置指导

13.1 静态路由配置指导

静态路由是在交换机设置的固定的路由表。除非网络管理员干预，否则静态路由不会发生变化。由于静态路由不能对网络的改变作出反映，一般用于网络规模不大、拓扑结构固定的网络中。静态路由的优点是简单、高效、可靠。

在对交换机进行路由配置时，可选择软件路由，也可选择硬件路由，硬件路由是指数据包不通过CPU直接硬件路由查找和转发。在配置静态路由时,若想硬件路由，则应该选择usehw选项（如下）。若用户配置了缺省路由（即0.0.0.0路由），并设置了硬件路由模式，若再配置其他网络路由，如再配置一条202.121.2.0/24的路由，还需配置对端相连接口的mac地址，本端相连的物理端口号，本端端口所在的VLAN号。

添加静态路由

【命令 1】 ip route static add *ipaddr netmask nexthopaddr* [description *string* usehw 〈*yes*/*no*〉 mac *mac-address* port *pnum* vid *vidnum*]

〖命令说明〗增加一条静态路由

〖参数说明〗“ipaddr” 是该目的子网地址，类型是A.B.C.D；

“netmask” 是子网掩码；

“nexthopaddr” 是下一跳地址；

“string”表示对该路由项的描述文字，用于标识记忆，该项可选；

usehw 表示该路由是否写入硬件，从而实现硬件三层转发；

*“mac_add” 表示对端相连接口的mac地址；

*“pnum”表示本端相连物理端口的端口号；

*“vidnum”表示相连物理端口所在的VLAN号；

注：* 号表示该选项在配置了缺省路由，并指定为硬件路由，在配置其他网络路由时会用到此选项。其他情况不用配置该选项。

[ ] 内的配置项是可选项；

〖命令模式〗配置模式

〖参考举例〗switch(config)# ip route static add 202.168.1.0 255.255.255.128 2.2.2.1 description testing usehw yes mac 00:08:93:da:00:04 port 2 vid 3

上述命令配置一条静态路由，目的子网是 202.168.1.0,子网掩码是 255.255.255.128,下一跳网关是 2.2.2.1,路由描述是 testing,该路由应用到硬件三层转发（usehw yes)。

☞ 在全局模式下，上述配置可以用 show ip route static 查看是否配置成功，若成功应显示含有下面信息：

Row	Dest Addr	Subnet Mask	Next Hop	Desc	UseHw	Status
1	202.168.1.0	255.255.255.128	2.2.2.2	testing	yes	nReady

删除静态路由

【命令 2】 ip route static delete *ipaddr*

〖命令说明〗删除一条静态路由

〖参数说明〗“ipaddr” 是该目的子网地址，类型是A.B.C.D;

〖命令模式〗配置模式

〖参考举例〗 switch(config)# ip route static del 202.168.1.0

上述命令删除去往 202.168.1.0 子网的静态路由。

WEB CONFIG 13.1-1

静态路由

静态路由配置

路由	目标地址	子网掩码	下一跳	描述	硬件方式?	网关?	状态
new	0.0.0.0	0.0.0.0	1.1.1.2		no	no	active
1	0.0.0.0	0.0.0.0	1.1.1.2		no	no	active

刷新 应用 删除

查看路由表

【命令 3】show ip route < dynamic | hardware | host | static | summary | table>

〖命令说明〗查看系统路由表

〖参数说明〗“dynamic” 表示查看动态路由表；

“hardware” 表示查看硬件路由表，即已经写到硬件的路由信息；

“host” 表示查看主机表路由；

“static” 表示查看静态路由；

“summary”表示查看路由表摘要，即整个路由表简化显示；

“table”　　表示查看整个路由表

〖命令模式〗全局模式

〖参考举例〗 switch# show ip route table

上述命令系统整个路由表。

13.2 RIP V1/V2协议配置指导

路由信息协议（Routing Information Protocol），简称为 RIP。它是基于距离矢量路由选择算法(Distance-Vector, D-V)的一种动态的内部网关协议(interior gateway protocol)，即在自治系统内部执行路由功能。

13.2.1 RIP协议介绍

RIP 协议报文承载在 UDP 协议上，它的端口号是 520。RIP 使用“跳数”来计算到目的网络的距离。RIP 规定最大跳数为 15，若跳数为 16 则表示网络不可达。

距离向量协议要求网内各个节点向自己所有的邻接点广播它对网内其它节点的可达性(用距离来衡量)，并通过逐级扩散的方式使这种可达性信息在网内传播，从而使各个节点能推算出自己到网内其它非邻接节点的路由。

路由信息协议主要包含两个版本RIP-1、RIP-2，其中版本2中增加支持明文认证和MD5 密文认证，并支持可变长子网掩码。由两个主要的文档中正式定义：RFC 1058和1723。RFC 1058(1988)描述了RIP的第一版实现，RFC 1723(1994)是它的更新，允许RIP分组携带更多的信息和安全特性。

RIP 协议的主要工作机制：

1. 初始化时，在每个运行 RIP 协议的接口上发送请求报文，运行 RIP 协议的相邻结点收到请求后，把整个路由表作为响应发送给请求者。
2. 接收到响应后，刷新本地的路由信息表中的内容。并向相邻的所有结点广播触发更新报文。
3. 每 30 秒路由器就把完整的路由表发送给相邻的路由器。
4. 为每一条路由条目关联相关的定时器，利用超时机制维护路由信息的实时性和有效性。

我们的产品的 RIP 功能特点主要有：

1. 支持触发更新
2. 支持 RIP-v1、RIP-v2 版本
3. 支持简单明文认证和 MD5 认证
4. 保持路由

13.2.2 配置RIP协议

在交换机上配置 RIP 协议包含以下内容：

- ✧ 打开或关闭 RIP 开关
- ✧ 在 IP 子网上运行 RIP 协议
- ✧ 设置 RIP 接口的相关参数

下面分别介绍设置上述参数的配置命令。

【命令1】router rip *enable/disable*

〖命令说明〗启动或关闭RIP路由协议
〖参数说明〗*enable启动RIP协议， disable关闭RIP协议*
〖命令模式〗配置模式
〖参考举例〗switch(config)# router rip *enable*
上述命令启用RIP协议

【命令2】route rip network *ipaddr*

〖命令说明〗在IP子网上起用RIP协议
〖参数说明〗*ipaddr*是要运行RIP的IP网络地址，类型为A.B.C.D
〖命令模式〗配置模式
〖参考举例〗switch(config)# route rip network 1.1.1.0
上述命令指定在子网1.1.1.0上运行RIP协议

【命令3】route rip no network *ipaddr*

〖命令说明〗在IP子网上禁用RIP协议
〖参数说明〗*ipaddr*是要运行RIP的IP网络地址，类型为A.B.C.D
〖命令模式〗配置模式
〖参考举例〗switch(config)# route rip no network 1.1.1.0
上述命令指定在子网1.1.1.0上禁用RIP协议

【命令4】 router rip entry *num* **authtype** *<noauth/simplepass/md5>*

〖命令说明〗配置运行RIP协议的接口num的验证方式。
〖参数说明〗“*num*”接口号，接口entry代表了属于该接口的所有物理接口， 认证类型authtype是可选参数，使用rip-v1时只能使用默认值"*noauth*"（无认证）； 使用rip-v2时可选择"*noauth*"（无认证）， "*simplepass*"（明文方式）， "*md5*"（*md5*加密方式）。
〖命令模式〗配置模式
〖参考举例〗 switch(config)# router rip entry 1 authtype noAuth
上述命令配置RIP路由协议在接口1上的验证方式为不使用验证(假设 entry 1 代表的是IP地址为2.2.2.2的接口)。

【命令5】router rip entry *num* **sendtype** *<doNotSend/ripVersion1/ripVersion2/ rip1compatible / ripv1demand / ripv2demand >*

〖命令说明〗配置运行RIP协议的接口num的路由信息的发送报文格式。
〖参数说明〗“*num*”接口号，接口entry代表了属于该接口的所有物理接口， 发送方式sendtype是可选参数，"*doNotSend*"(不发送路由报文)；"*ripVersion1*"（RIP协议1的报文格式），"*ripVersion2*"（RIP协议2的报文格式）*rip1compatible*（RIP协议1兼容报文格式），*ripv1demand*（RIP协议1的查询报文），*ripv2demand*（RIP协议2的查询报文）。
〖命令模式〗配置模式
〖参考举例〗 switch(config)# router rip entry 1 sendtype ripVersion2
上述命令配置RIP路由协议在接口1上的发送报文方式为RIP协议2的报文格式(假设entry 1 代表的是IP地址为2.2.2.2的接口)。

【命令6】router rip entry *num* recvtype *<rip1/rip2/rip1OrRip2/doNotReceive>*

〖命令说明〗配置运行RIP协议的接口num的路由信息的接收报文格式。
〖参数说明〗“*num*”接口号，接口entry代表了属于该接口的所有物理接口， 接收方式recvtype是可选参数，"*rip1*"(RIP协议1的报文格式)；"*rip2*"（RIP协议2的报文格式），"*rip1OrRip2*"（RIP协议1或2的报文格式），"*doNotReceive*"（不接收RIP任何报文）。
〖命令模式〗配置模式
〖参考举例〗 switch(config)# router rip entry 1 recvtype rip2
上述命令配置RIP路由协议在接口1上的接收报文格式为RIP协议2的报文格式(假设entry 1 代表的是IP地址为2.2.2.2的接口)。

【命令7】router rip entry *num* metric *intval*

〖命令说明〗配置运行RIP协议的接口num的路由权值。
〖参数说明〗“*num*”接口号，接口entry代表了属于该接口的所有物理接口，路由权值metric，intval的范围为1-15。
〖命令模式〗配置模式
〖参考举例〗 switch(config)# router rip entry 1 metric 2
上述命令配置RIP路由协议在接口1上的路由权值为2（假设entry 1 代表的是IP地址为2.2.2.2的接口)。

【命令8】router rip entry *num* password *<string(0-16)>*

〖命令说明〗配置运行RIP协议的接口num的认证的口令。
〖参数说明〗“*num*”接口号，接口entry代表了属于该接口的所有物理接口，可选的认证口令password，范围是0-16长度的字符串，可用于明文及md5验证方式。
〖命令模式〗配置模式

〖参考举例〗 switch(config)# router rip entry 1 password 123456
上述命令配置RIP路由协议在接口1上的认证口令为“123456”（假设entry 1 代表的是IP地址为2.2.2.2的接口）。

13.3 OSPF协议配置指导

OSPF即开放最短路径优先协议（Open Shortest Path First），它是Internet Engineering Task Force（IETF）的IGP（88年成立，专门研究域内路由协议）工作组于90年代初提出的。OSPF协议的最新版本是1998年公布的OSPFv2（RFC 2178）。

13.3.1 OSPF协议介绍

OSPF是一种基于链路状态的路由协议，它要求各结点发送自己的链路状态（Link StateAdvertisement－LSA）到同一层次区域（area）的所有其它结点。LSA中包括结点的邻接情况，所使用的测度等，这样区内各结点便逐渐掌握了全网的拓扑情况，并以此使用Dijkstra最短路径算法（也称为SPF算法）来产生最短路径树，它代表了从该结点到区内其他各结点的最短路径。以IP报文的形式交换OSPF协议路由信息。

OSPF把一个大型网络分割成多个小型网络的能力被称为分层路由，这些被分割出来的小型网络 就称为“区域”(Area)。由于区域内部路由器仅与同区域的路由器交换LSA信息，这样LSA报文数量及链路状态信息库表项（LSDB）都会极大减少，SPF计算速度因此得到提高。多区域的OSPF必须存在一个主干区域，主干区域负责收集非主干区域发出的汇总路由信息，并将这些信息返还给到各区域。

OSPF协议的优点

1. 通过设置区域Area，分层路由等使OSPF协议能支持更大型的网络拓扑结构。
2. 相对于RIP等使用基于VD算法的路由协议，OSPF区域之间及不同区域之间所占用的通信量带宽极大地减少，避免了广播风暴。
3. 收敛速度快，当路由发生变化时，SPF能更快达到新的稳定状态。
4. 使用链路状态的算法，杜绝了路由自环的弊端。

注意：

在与CISCO路由器或交换机通过OSPF协议互联时，需要在CISCO路由器或交换机上关`闭其opaque能力，操作命令为：switch(config-router)#no capability opaque。

13.3.2 配置OSPF协议

启动或关闭 OSPF 开关

【命令1】 service *enable*|*disable*

〖命令说明〗启动关闭OSPF路由协议
〖参数说明〗无
〖命令模式〗路由配置模式
〖参考举例〗switch(router-ospf)# service enable
上述命令配置交换机使用OSPF协议

配置路由器 ID 号

【命令1】 router-id *<A.B.C.D>*

〖命令说明〗在OSPF协议配置模式下，配置路由器ID号

〖参数说明〗*<A.B.C.D>*交换机接口IP地址

〖命令模式〗路由配置模式

〖参考举例〗switch(router-ospf)# router-id 1.1.1.1

上述命令配置交换机ID为1.1.1.1

注意:

缺省情况下，路由器选择其所有接口中的最小 IP 地址作为其路由器 ID 号。

定义参与 ospf 的子网

【命令1】 network *ipaddr netmask* area *areaid*

〖命令说明〗定义参与ospf的子网

〖参数说明〗"*ipaddr* "子网IP地址，类型为A.B.C.D；" *netmask*"子网掩码 ；"*areaid*" 路由区域ID，类型为0-4294967295或A.B.C.D

〖命令模式〗路由配置模式

〖参考举例〗switch(router-ospf)# network 1.1.1.0 255.255.255.0 area 0

上述命令在子网1.1.1.0上启用OSPF协议，区域ID为0。

设置发送 Hello 报文的时间间隔

【命令1】 ip ospf hello-interval *<1-65535>*

〖命令说明〗设置接口发送Hello报文的时间间隔

〖参数说明〗*<1-65535>*，发送hello报文的间隔时间，单位是秒

〖命令模式〗接口配置模式

〖参考举例〗switch(config-if)# ip ospf hello-interval 15

上述命令设置接口发送Hello报文的时间间隔为15秒。

注意:

缺省情况下，接口发送 Hello 报文的时间间隔为 10 秒。

配置 OSPF 接口的邻居路由器的死亡时间间隔

【命令 1】 ip ospf dead-interval *<1-65535>*

〖命令说明〗设置邻居路由器的死亡时间间隔

〖参数说明〗*<1-65535>*，邻居路由器的死亡时间间隔，单位是秒

〖命令模式〗接口配置模式

〖参考举例〗switch(config-if)# ip ospf dead-interval 50

上述命令设置邻居路由器的死亡时间间隔为50秒。

注意:

缺省情况下，邻居路由器的死亡时间间隔为 40 秒。

设置 OSPF 接口的 LSA 传输延迟时间

【命令1】 ip ospf transmit-delay *<1-65535>*
〖命令说明〗设置LSA传输延迟时间
〖参数说明〗*<1-65535>*，LSA传输延迟时间，单位是秒
〖命令模式〗接口配置模式
〖参考举例〗switch(config-if)# ip ospf transmit-delay 50
上述命令设置LSA传输延迟时间为50秒。

注意：
缺省情况下，LSA 传输延迟时间为 40 秒。
恢复出厂默认 LSA 传输延迟用命令：no ip ospf transmit-delay

设置 OSPF 接口重传 LSA 的时间间隔

【命令1】 ip ospf retransmit-interval *<3-65535>*
〖命令说明〗设置重传LSA的时间间隔
〖参数说明〗*<3-65535>*，重传LSA的时间间隔，单位是秒
〖命令模式〗接口配置模式
〖参考举例〗switch(config-if)# ip ospf retransmit-interval 10
上述命令设置重传LSA的时间间隔为10秒。

注意：
缺省情况下，重传 LSA 的时间间隔为 5 秒。
恢复出厂默认 LSA 传输延迟用命令：no ip ospf retransmit-interval

设置 OSPF 接口的优先级

【命令1】 ip ospf priority *<0-255>*
〖命令说明〗设置接口在选举指定路由器时的优先级
〖参数说明〗*<0-255>*接口在选举指定路由器时的优先级
〖命令模式〗接口配置模式
〖参考举例〗switch(config-if)# ip ospf priority 2
上述命令设置接口在选举指定路由器时的优先级为2

注意：
缺省情况下，缺省情况下接口在选举 DR 时的优先级取值为 1
恢复出厂默认优先级用命令：no ip ospf priority

配置 OSPF 协议的被动接口

【命令1】 ip ospf passive
〖命令说明〗在接口配置模式下，配置被动接口
〖参数说明〗无
〖命令模式〗接口配置模式

〖参考举例〗switch(config-if)# ip ospf passive

上述命令设置所进入的接口为被动接口。

注意：

缺省情况下，系统没有配置被动接口

恢复出厂默认用命令：no ip ospf passive

配置 OSPF MD5 验证信息

【命令1】 ip ospf authentication-md5 *<1-255>* *<key_string>*

〖命令说明〗配置接口的MD5验证

〖参数说明〗<1-255>是由用户输入的key-id号，<key_string>是由用户输入的最大为16位字符串密码

〖命令模式〗接口配置模式

〖参考举例〗switch(config-if)# ip ospf authentication-md5 1 test

上述命令设置接口MD5认证密码为test

注意：

缺省情况下，接口将不对报文进行验证。

恢复出厂默认或取消认证用命令：no ip ospf authentication-md5

配置 OSPF 简单验证信息

【命令1】 ip ospf authentication-simple *<key_string>*

〖命令说明〗配置接口的MD5验证

〖参数说明〗<key_string>是由用户输入的最大为8位字符串密码

〖命令模式〗接口配置模式

〖参考举例〗switch(config-if)# ip ospf authentication-simple test

上述命令设置接口简单认证密码为test

注意：

缺省情况下，接口将不对报文进行验证。

恢复出厂默认或取消认证用命令：no ip ospf authentication- simple

配置接口发送报文的花费

【命令1】 ip ospf cost *<1-65535>*

〖命令说明〗配置接口发送报文的花销

〖参数说明〗*<1-65535>*，接口发送报文的花销

〖命令模式〗接口配置模式

〖参考举例〗switch(config-if)# ip ospf cost 2

上述命令设置接口发送报文的花销为2。

注意：

缺省情况下，接口发送报文的花销为 1。
恢复出厂默认接口发送报文的花销用命令：no ip ospf cost

配置 OSPF 的 STUB 区域

【命令1】 area *areaid* stub [no-summary]
〖命令说明〗配置OSPF的STUB区域
〖参数说明〗“*areaid*” OSPF区域ID，类型为A.B.C.D或0-4294967295之间的整数
〖命令模式〗路由配置模式
〖参考举例〗switch(router-ospf)# area 1 stub
上述命令设置OSPF 区域1 为STUB域。

注意：
缺省情况不配置 Stub 区域。
恢复出厂默认用命令：no area *areaid* stub

配置到 STUB 区域的默认花费

【命令1】 area *<A.B.C.D>*/ *<0-4294967295>* default-cost *<0-65535>*
〖命令说明〗配置到STUB区域的默认花费
〖参数说明〗*<A.B.C.D>* 点分十进制表示的OSPF区域ID，*<0-4294967295>整数*表示的OSPF区域ID，*<0-65535>*用户输入的所配置的默认花费值
〖命令模式〗路由配置模式
〖参考举例〗switch(router-ospf)# area 1 default-cost 10
上述命令设置到STUB区域的默认花费为10

注意：
缺省情况不到 STUB 区域的默认花费为 10。
取消到 STUB 区域的默认花费用命令：no area *<A.B.C.D>*/ *<0-4294967295>* default-cost *<0-65535>*

配置 OSPF 区域间路由聚合

【命令1】 area *<A.B.C.D>*/ *<0-4294967295>* *ipaddr netmask*
〖命令说明〗配置OSPF区域间路由聚合
〖参数说明〗*<A.B.C.D>* 点分十进制表示的OSPF区域ID，*<0-4294967295>整数*表示的OSPF区域ID，“*ipaddr*” 需要配置聚合成某一个网段的网段地址，类型为A.B.C.D；“*netmask*”子网掩码，类型为A.B.C.D
〖命令模式〗路由配置模式
〖参考举例〗switch(router-ospf)# area 1 range 1.1.0.0 255.255.0.0
上述命令设置对区域1进行路由聚合

注意：
缺省情况下不进行区域路由聚合

取消区域路由聚合用命令：no area *<A.B.C.D>/ <0-4294967295> ipaddr netmask*

配置 OSPF 虚连接

【命令1】 area *<A.B.C.D>/<0-4294967295> routerid* [hello-interval|retransmit-interval|transmit-delay|dead-interval] <1-65535> [authentication-simple] <key_string> [authentication-md5] <1-255> <key_string>

〖命令说明〗配置OSPF虚连接

〖参数说明〗 *"routerid"* 远端ABR域的路由器的ID，类型为A.B.C.D；

〖命令模式〗路由配置模式

注意：

缺省情况下不创建虚连接。

取消虚连接用命令：no area *<A.B.C.D>/<0-4294967295> routerid* [hello-interval|retransmit-interval|transmit-delay|dead-interval] <1-65535> [authentication-simple] <key_string> [authentication-md5] <1-255> <key_string>

配置转发路由信息

【命令1】 redistribute [connected|static|rip|bgp] [metric] *<0-16777214>* [type-metric] *<1-2>* [tag] *<0-2147483647>*

〖命令说明〗配置转发路由信息，OSPF将所有引入自治系统中的路由当作外部路由，它们描述了应该如何选择到自治系统以外目的地的路由，自治系统的外部路由包括第一类外部路由(Type 1) 和第二类外部路由(Type 2)，它们在路由表中的优先级也是相同的(缺省为150)。

〖参数说明〗

〖命令模式〗路由配置模式

注意：

缺省情况下 OSPF 不引入其它协议的路由信息

取消配置转发路由信息用命令：no redistribute [connected|static|rip|bgp] [metric] *<0-16777214>* [type-metric] *<1-2>* [tag] *<0-2147483647>*

配置转发路由的汇总

【命令1】 summary-address *ipaddr netmask* [not-advertise] [tag] *<0-2147483647>*

〖命令说明〗配置转发路由的汇总网络

〖参数说明〗not-advertise 是指不洪泛落入此范围的路由，Tag是指此汇总网络路由的标记

〖命令模式〗路由配置模式

注意：

缺省情况下洪泛汇总网络路由。

取消所配置的转发路由的汇总网络用命令：no summary-address *ipaddr netmask*

配置 OSPF 协议的定时器

【命令1】 timers spf *<0-4294967295> <0-4294967295>*

〖命令说明〗配置OSPF协议的定时器

〖参数说明〗第一个<0-4294967295> 数值是配置接收改变到最短路径计算之间的延迟。第二个<0-4294967295> 数值是配置连续最短路径计算之间的保持时间。

〖命令模式〗路由配置模式

OSPF 的监控和维护

【命令1】 show ip ospf

〖命令说明〗显示OSPF 主要信息

〖参数说明〗

〖命令模式〗全局模式

【命令2】 show ip ospf routing

〖命令说明〗显示OSPF路由信息

〖参数说明〗

〖命令模式〗全局模式

【命令3】 show ip ospf routing abr

〖命令说明〗显示OSPF区域边界路由信息

〖参数说明〗

〖命令模式〗全局模式

【命令4】 show ip ospf routing area *<A.B.C.D>|<0-4294967295>*

〖命令说明〗显示ospf区域路由信息

〖参数说明〗

〖命令模式〗全局模式

【命令5】 show ip ospf routing asbr

〖命令说明〗显示OSPF自治系统边界路由信息

〖参数说明〗

〖命令模式〗全局模式

【命令6】 show ip ospf virtual-links

〖命令说明〗显示OSPF虚链路信息

〖参数说明〗

〖命令模式〗全局模式

【命令7】 show ip ospf neighbo

〖命令说明〗显示OSPF邻居信息

〖参数说明〗

〖命令模式〗全局模式

【命令8】show ip ospf interface [vint] *<0-31>*

〖命令说明〗显示OSPF接口信息

〖参数说明〗

〖命令模式〗全局模式

【命令9】 show ip ospf database

〖命令说明〗显示OSPF数据库中的所有路由信息

〖参数说明〗

〖命令模式〗全局模式

【命令10】 ip ospf database adv-router *<A.B.C.D>*

〖命令说明〗显示某一路由器产生的路由信息

〖参数说明〗

〖命令模式〗全局模式

【命令11】 show ip ospf database area *<A.B.C.D>|<0-4294967295>*

〖命令说明〗显示某一区域数据库路由信息

〖参数说明〗

〖命令模式〗全局模式

【命令12】 show ip ospf database database-summary

〖命令说明〗显示所有区域中的网络汇总链路状态通告路由信息

〖参数说明〗

〖命令模式〗全局模式

【命令13】 show ip ospf lsa

〖命令说明〗显示所有的OSPF链路状态通告信息

〖参数说明〗

〖命令模式〗全局模式

【命令14】show ip ospf lsa area *<A.B.C.D>|<0-4294967295>*

〖命令说明〗显示某一区域的链路状态通告信息

〖参数说明〗

〖命令模式〗全局模式

【命令15】show ip ospf lsa summary

〖命令说明〗显示网络汇总链路状态通告信息
〖参数说明〗
〖命令模式〗全局模式

第 14 章 配置 IGMP 和组播路由协议

三层交换机同时具备二层组播（如IGMP SNOOPING等）和三层组播功能。三层交换机本身具备动态组播路由协议，负责组播路由的建立和组播数据的转发。
组播是一种点到多点的通信方式。IP组播报文的目的地址是一个 D类 IPv4地址(即从224.0.0.0至239.255.255.255)。它实际上已经不是某个设备的 IP地址，而是表示一个组。其中 224.0.0.*/24和 239.0.0.*/24这两个段一般是被协议保留，不能用于用户数据通讯。

三层交换机目前支持 IGMP协议和 PIM-SM协议，二者配合可以有效支持 IP组播应用。其中IGMP协议用于获得某个网段上是否有终端设备需要接收某个组的报文，而 PIM-SM协议则用于在网络上计算组播路由，建立组播转发路径。
三层组播与二层组播的主要区别在于它使用 IP组播路由协议，从而可以在跨越多个三层设备，在多个网段之间选择组播转发路由，控制组播数据有效地转发到需要数据的网段，避免转发到不需要的网段，并可以抑制数据重复转发到一个网段上。
三层组播的上层应用通常包括：视频点播、视频会议、远程教学、电子白板、数据公告（如股市行情）等。
本章包括如下内容：
✧ 三层组播基本配置指导
✧ IGMP 协议配置指导
✧ PIM-SM V2协议配置指导
配置前，需要对IP组播机制有一个全面的了解，可参考以下资料：
RFC 1112 —— Internet Group Management Protocol（IGMP）, Version 1
RFC 2236 —— Internet Group Management Protocol（IGMP）, Version 2
RFC 2362 —— Protocol Independent Multicast-Sparse Mode (PIM-SM) Protocol Specification

14.1 基本配置命令

14.1.1 打开或关闭组播路由开关

交换机中 IP 组播路由转发功能缺省状态是关闭的。设定 IP 组播路由转发功能开启和关闭，利用命令：

【命令1】ip multicast-routing *<enable/disable>*

〖参数说明〗enable表示开启IP组播路由开关，disable表示关闭IP组播路由开关。在启动组播路由协议或IGMP协议之前，要先通过这个命令启动组播转发功能。
〖命令模式〗配置模式
〖参考举例〗

- 开启 IP 组播开关

switch(config)# ip multicast-routing enable
上述操作启动 IP 组播转发功能。

- 关闭 IP 组播开关

  switch(config)# ip multicast-routing disable

  上述操作停止IP组播转发功能。

☞ 在全局模式下键入show ip mroute查看是否设置成功，即：

```
switch# show ip mroute
IP Multicast Forwarding : Enabled
```

14.1.2 显示组播路由表条目

要查看组播路由表。利用命令：

【命令1】show ip mroute

〖参数说明〗无。显示整个组播路由表。

〖命令模式〗全局模式

14.2 IGMP协议及其配置

IGMP(Internet Group Management Protocol)的功能是管理组播成员信息。该协议一般运行在组播域中直接与接收者连接的设备上，它动态的建立、维护组播组成员关系，是组播路由体系中的基础协议。

目前常用的 IGMP 协议有两个版本：IGMP v1 和 IGMP v2。本系统在全面实现 IGMP v2 的基础上，考虑到向下兼容性问题，可以接收 IGMP v1 的报文，但不发送 IGMP v1 报文。

IGMP v2 有 3 种主要报文

1. Memebership Query：是运行 IGMP 协议的 Internet Group Management Protocol 发送给组播接收者（主机）的，根据报文中组播组地址的不同，分为常规查询和特定组查询。当查询报文中的组播组地址为 0.0.0.0 时，用于确定当前的接口所在的网段上存在哪些组播组的接收者；当组播组地址为特定的合法组播组地址时，用于确定当前接口所在的网段上是否存在该组的接收者。
2. Memebership Report：是支持 IGMP 协议的主机向组播路由设备汇报网络上存在特定组播组的活动成员时使用的报文。本系统支持两种报告报文：版本 1 和版本 2 的成员报告。
3. Leave Group：当主机离开一个组播组时，向所有组播路由器发送一个成员离开报文。

IGMP 配置的步骤是：

(1) 在配置模式下启动组播：配置命令为 ip multicast-routing

(2) 在相关的接口上启动 IGMP：在接口上启动 IGMP。通过启动 PIM 等组播协议，IGMP 协议会自动地随组播路由协议而启动。

(3) 加入组播组：有两种方式：动态和静态加入。动态加入不需配置，通过接收者发送 IGMP Memebership Report 报文实现；静态配置一般是为了保证在特定接口上有一个稳定的流输出，配置方法是在特定接口下使用 ip igmp static-group 命令

14.2.1 启动/禁用IGMP协议

配置交换机接口，启动/禁用 IGMP 和 PIM-SM 协议。利用命令：

【命令1】 ip pim interface <*ifname*> sparse-mode <*enable|disable*>

〖参数说明〗*ifname* 接口名，例如 vint 0；
〖命令模式〗配置模式
〖参考举例〗

- 使 Vint 接口 0 启用 IGMP 协议：
  switch(config)# ip pim interface vint 0 sparse-mode enable
  上述操作使 Vint 接口 0 同时启用 IGMP v2 和 PIM v2 协议。

14.2.2 配置交换机接口成为组成员

配置交换机接口成为组播组成员，可使交换机加入组播组。利用命令：

【命令1】 ip igmp interface <*ifname*> join-group <*group*>
【命令2】 ip igmp interface <*ifname*> leave-group <*group*>

〖参数说明〗*ifname* 接口名，例如 vint 0；
group IGMP组地址 点分格式(A.B.C.D)。
〖命令模式〗配置模式
〖参考举例〗

- 使 Vint 接口 0 成为组播地址 225.1.1.1 的成员：
  switch(config)# ip igmp interface vint 0 join-group 225.1.1.1
  上述操作使 Vint 0 接口属于组播地址为 225.1.1.1 的成员。

14.2.3 配置交换机当前的IGMP静态成员

增加/删除当前交换机某接口的 IGMP 成员。利用命令：

【命令1】 ip igmp interface <*ifname*> static-group add <*group*>
【命令2】 ip igmp interface <*ifname*> static-group delete <*group*>
〖参数说明〗*group* IGMP组地址 点分格式(A.B.C.D)，*ifname* 接口名。
〖命令模式〗配置模式
〖参考举例〗

- 增加一组播地址成员：
  switch(config)# ip igmp interface vint 0 static-group add 225.1.1.1
  上述操作对 Vint 0 接口增加属于组播地址为 225.1.1.1 的成员。

☞ 在全局模式下键入show ip igmp group <*interface*>查看配置，即：

switch# show ip igmp group vint 0

14.2.4 配置交换机接口运行IGMP的版本号

同一子网上的所有系统应支持相同的 IGMP 版本，但交换机不能自动检测接口当前运行的 IGMP 版本号。缺省情况下，交换机接口运行 IGMP Version 2。

【命令1】ip igmp interface 〈*ifname*〉 version 〈*1/2*〉

〖参数说明〗*ifname* 接口名。

〖命令模式〗配置模式

〖参考举例〗

- 配置交换机接口 Vint 0：
  switch(config)# ip igmp interface vint 0 version 1
  上述操作对配置 Vint 0 接口上运行 IGMP 1。

☞ 在全局模式下键入show ip igmp groups 〈*interface*〉查看配置，即：

switch# show ip igmp groups vint 0

14.2.5 配置IGMP查询超时时间

IGMP 查询者超时时间用于网段上有多个 IGMP 路由器时，它们之间要竞争由谁发出 IGMP 查询报文。竞争结果的有效时间就是这个查询者超时时间。即非查询者路由器过了这么长时间没有收到查询报文，就会认为查询者已经退出，将再次发出查询报文，并以此竞争查询者。按协议规定，查询者超时时间为可靠系数*查询间隔+响应时间/2，缺省为 2*125+10/2 秒，即 255 秒。注意，查询间隔是可以配置的。当查询时间被修改后，查询者超时时间会按这个公式重新计算，可能会不再是原来配置的查询者超时时间。利用命令：

【命令1】ip igmp querier-timeout 〈*60-300*〉

〖参数说明〗<60-300>IGMP查询者超时时间（秒）。IGMP查询者超时时间缺省为255秒。

〖命令模式〗配置模式

〖参考举例〗

- 设置查询者超时时间
  switch(config)# ip igmp querier-timeout 200
  上述操作设置查询者超时时间为 200 秒。

14.2.6 配置IGMP查询间隔

IGMP 查询间隔是协议的一个重要参数，它控制着 IGMP 发出查询的频率，同时也影响其它一些系统时间参数，如成员超时时间=可靠系数*查询间隔+响应时间，查询者超时时间=可靠系数*查询间隔+响应时间/2。配置交换机 IGMP 查询间隔。利用命令：

【命令1】ip igmp query-interval 〈*1-65535*〉

〖参数说明〗<1-65535> IGMP查询间隔（秒）。IGMP查询间隔缺省为125秒。

〖命令模式〗配置模式

〖参考举例〗

- 配置 IGMP 查询间隔
  switch(config)# ip igmp query-interval 120
  上述操作配置 IGMP 查询间隔为 120 秒。

14.2.7 IGMP的监控与维护

这些命令主要查看交换机的状态和配置。

组成员查看命令显示内容包括 IGMP 协议收到的组成员加入信息，以及通过静态组成员配置命令加入的成员信息。静态信息无论目前是否生效都可以显示，并说明了当前状态。如果不使用参数，则显示当前的所有 IGMP 成员信息。如果输入接口名称参数，则显示该接口上的当前 IGMP 成员信息。

接口命令用来显示 IGMP 接口的配置信息：包括协议状态，各种定时器得值，选举出的查询者等。

利用命令：

【命令1】show ip igmp groups interface 〈*ifname*〉
【命令2】show ip igmp interface 〈*ifname*〉〉
〖参数说明〗〈*ifname*〉 接口名称。
〖命令模式〗全局模式
〖参考举例〗

- 查 Vint 0 接口的信息
  switch(config)# show ip igmp interface vint 0
  上述操作显示 Vint 0 接口上的配置和状态。

14.3 组播路由协议PIM-SM v2的配置

PIM(Protocol Independent Multicast)协议是一种独立于单播路由协议的组播协议，按照应用场合和处理机制的不同，可以分为密集模式(Dense Mode)和稀疏模式(Sparse Mode)两种。密集模式适合于组播源和接收者物理距离近、数据报文流量大而且持续、接收者密度较大的网络，典型的例子是局域网；稀疏模式适合于组播发送源和组播接收者分布在较大范围且带宽受限的网络中，如 Internet。

PIM-SM 配置的步骤
(1) 启动组播：在配置模式下执行命令 ip multicast-routing
(2) 在接口上启动组播：同时启动 PIM 等组播协议和 IGMP 协议。
(3) 指定集中点（RP）：使用 Bootstrap 动态发布的方式。需要指定 BSR 和候选 RP：在一个组播域中必须保证至少有一个激活的候选 BSR，对每个组播组必须保证至少存在一个可以映射到的 RP。配置方法是选定的设备上，在配置模式下运行 ip pim bsr-candidate 和 ip pim rp-candidate 命令。

14.3.1 启动PIM-SM协议

将接口加入三层组播转发有两种方式：启动 PIM 等组播协议和 IGMP，或只启动 IGMP 协议。本命令在对应的接口上启动 PIM-SM 协议和 IGMP 协议。使用 PIM 协议必须通过此命令在至少 1 个接口上启动 PIM 协议。利用命令：

【命令1】ip pim interface 〈*ifname*〉 sparse-mode 〈*enable*/*disable*〉

〖参数说明〗interface 接口名。enable 和 disable分别启动和关闭接口IGMP和PIM

协议。

〖命令模式〗配置模式

〖参考举例〗

- 配置交换机

  switch(config)# ip pim interface vint 0 sparse-mode enbable

  上述操作对交换机 Vint 0 接口启动 PIM-SM 协议。

在全局模式下键入show ip pim interface查看接口组播配置参数，即：

switch# show ip pim interface vint 0

14.3.2 配置候选bsr(bootstrap router)

BSR（Bootstrap Router）是 PIM 网络中的启动消息（bootstrap）发出者。在 PIM 网络中必须存在一个唯一的 BSR 设备。它接受候选 RP 的消息通告，并发出 bootstrap 把当前的 RP 表通知给域中的所有路由器。在 PIM 网络中，必须通过这个命令配置至少一个候选 BSR。利用命令：

【命令1】ip pim bsr-candidate 〈*ifname*〉 {**priority** 〈*priority*〉}

〖参数说明〗ifname 选择候选BSR的IP地址的接口名。priority候选BSR竞争BSR的优先级，范围<0-255>缺省为0(最小)。

〖命令模式〗配置模式

〖参考举例〗

- 配置交换机的某一接口为 BSR：

  switch(config)# ip pim bsr-candidate vint 0

  上述操作配置 Vlan 0 端口为侯选 BSR。



在全局模式下键入show ip pim interface vint x查看配置，即：

switch# show ip pim interface vint 0

14.3.3 配置PIM候选RP

配置本机接口为 PIM 侯选 RP。利用命令：

【命令1】ip pim rp-candidate 〈*ifname*〉 {**priority** 〈*priority*〉}

〖参数说明〗*interface* 选择候选RP IP地址的接口名称 。在PIM网络中，必须通过这个命令配置至少一个候选RP。priority候选RP竞争RP的优先级，范围<0-255>缺省为0(最小)。

〖命令模式〗配置模式

〖参考举例〗

- 配置交换机接口 Vint 0 为侯选 RP

  switch(config)# ip pim rp-candidate vint 0

  上述操作设置交换机 Vint 0 接口为侯选 RP。

☞ 在全局模式下键入show ip pim interface vint x 查看配置参数，即：

switch# show ip pim interface vint 0

14.3.4 配置PIM HELLO消息发送间隔

配置 PIM 的 HELLO 消息发送间隔。利用命令：

【命令1】ip pim query-interval *<0-65535>*

〖参数说明〗<0-65535>　HELLO消息发送间隔（以秒为单位，默认值为30秒）。
〖命令模式〗配置模式
〖参考举例〗

- 配置交换机 HELLO 消息发送间隔
  switch(config)# ip pim query-interval 40
  上述操作设置交换机 PIM HELLO 消息发送间隔为 40 秒。

☞ 在全局模式下键入show ip pim interface vint x 查看配置参数，即：

switch# show ip pim interface vint 0

14.3.5 设置从共享树切换到源最短路径树的阈值

PIM-SM 交换机最初通过共享树转发组播报文，但是如果组播数据通过的速率超过一定的阈值，组播报文所经过的最后一跳交换机就会发起从共享树到最短路径树的切换过程。缺省情况下，从共享树切换到源最短路径树的阈值为 0，也就是说当最后一跳交换机收到第一个组播报文后立即切换到最短路径树。

【命令1】ip pim spt-threshold *<0-4294967>*

〖参数说明〗<0-4294967> 单位为kbits/s。
〖命令模式〗配置模式

14.3.6 显示PIM协议的BSR选择信息

此命令显示当前采用的 BSR 地址、优先级、RP 映射掩码等信息。

【命令1】show ip pim bsr-router

〖参数说明〗
〖命令模式〗全局模式

14.3.7 显示运行PIM的接口信息

显示运行 PIM 的接口表和相应的状态。利用命令：

【命令1】show ip pim interface *<ifname>*

〖参数说明〗*ifname* 接口名称。
〖命令模式〗全局模式

14.3.8 显示PIM邻居信息

显示交换机 PIM 邻居信息。此命令显示协议当前已经获得的 PIM 邻居情况。PIM 邻居是通过 HELLO 报文发现的。不带参数时，将显示所有的 PIM 邻居信息；带接口名称参数时，显示特定接口上的 PIM 邻居。利用命令：

【命令1】show ip pim neighbor

〖参数说明〗
〖命令模式〗全局模式
〖参考举例〗

- 显示接口 Vint 0 的 PIM 邻居信息
  switch(config)# show ip pim neighbor

☞ 在全局模式下键入show ip pim neighbour查看配置参数，即：

switch# show ip pim neighbour

14.3.9 显示当前RP列表

显示交换机当前的 RP 列表。利用命令：

【命令1】show ip pim rp

〖参数说明〗此命令显示的内容包括两部分：当前获得的RP列表（包括RP地址、管理的组地址范围、来源、超时时间等）以及该设备上的组播组与RP的映射表。
〖命令模式〗全局模式

14.3.10 查询组RP映射

查询交换机一个组的 RP 映射结果。利用命令：

【命令1】show ip pim rp-info *A.B.C.D*

〖参数说明〗可通过命令计算任意一个组的RP映射，了解系统中对RP的选择。
〖命令模式〗全局模式
〖参考举例〗

-
  switch(config)# show ip pim rp-hash 225.1.1.1
  上述操作显示交换机组地址为 225.1.1.1 的 RP 映射。

第 15 章 配置 802.1x

IEEE 802.1x 称为基于端口的访问控制协议（Port based network access control protocol）。它的协议体系结构包括三个重要的部分：客户端系统（Supplicant System）、认证系统（Authenticator System）、认证服务器（Authentication Server System）。

15.1 打开或关闭802.1x认证开关

交换机中 802.1x 认证缺省状态是关闭的。设定 802.1x 认证开启和关闭，利用命令：

【命令1】dot1x system-auth-control *<enable/disable>*

〖参数说明〗enable表示开启802.1x认证开关，disable表示关闭802.1x认证开关。
〖命令模式〗配置模式
〖参考举例〗

- 开启 802.1x 认证开关
  switch(config)# dot1x system-auth-control enable
  上述操作打开 802.1x 认证开关。

- 关闭 802.1x 认证开关
  switch(config)# dot1x system-auth-control disable
  上述操作关闭802.1x认证开关。

☞ 在全局模式下键入show dot1x system-auth-control查看是否设置成功，即：
switch# show dot1x system-auth-control

WEB CONFIG 15.1-1



15.2 配置端口的认证控制状态

交换机中端口的认证控制状态缺省状态是所有端口都关闭。设定端口的认证控制状态开启和关闭，利用命令：

【命令1】dot1x ports *String*

〖参数说明〗*“String”定义参与认证的端口*

<port number>m表示开启802.1x端口认证，<port number>-表示关闭802.1x端口认证。

〖命令模式〗配置模式

〖参考举例〗

- 开启 5、18 端口认证，关闭 1、20 端口认证
  switch(config)# dot1x ports 01-05m18m20-
  上述操作配置端口的认证控制状态。

☞ 在全局模式下键入show dot1x ports查看端口的认证控制状态，即：

switch# show dot1x ports

15.3 配置802.1x认证端口允许通过的主机数目

交换机中 802.1x 认证端口允许通过的主机数目缺省值是 256（最大值）。设定 802.1x 认证端口允许通过的主机数目，利用命令：

【命令1】dot1x multiple-host-num *Number*

〖参数说明〗输入整数型数值，注意范围为1～256。

〖命令模式〗配置模式

〖参考举例〗

- 配置 802.1x 认证端口允许通过的主机数目为 10
  switch(config)# dot1x multiple-host-num 10
  上述操作配置 802.1x 认证端口允许通过的主机数目。

☞ 在全局模式下键入show dot1x multiple-host-num查看802.1x认证端口允许通过的主机数目，即：

switch# show dot1x multiple-host-num

第 16 章 配置 WEB/Portal 认证

Web/Portal认证是基于业务类型的认证，不需要安装其他客户端软件，只需要浏览器就能完成，就用户来说较为方便。Web/Portal认证尤其适合在酒店等网络环境中使用。

16.1 打开或关闭WEB/Portal认证开关

交换机中 WEB/Portal 认证缺省状态是关闭的。设定 WEB/Portal 认证开启和关闭，利用命令：

【命令1】 webportal system-auth-control *<enable/disable>*

〖参数说明〗enable表示开启web/Portal认证开关，disable表示关闭web/Portal认证开关。

〖命令模式〗配置模式

〖参考举例〗

- 开启 web/Portal 认证开关
  switch(config)# webportal system-auth-control enable
  上述操作打开 web/Portal 认证开关。

- 关闭 web/Portal 认证开关
  switch(config)# webportal system-auth-control disable
  上述操作关闭web/Portal认证开关。

在全局模式下键入show webportal system-auth-control查看是否设置成功，即：

switch# show webportal system-auth-control

16.2 配置端口的认证控制状态

交换机中端口的认证控制状态缺省状态是所有端口都关闭。设定端口的认证控制状态开启和关闭，利用命令：

【命令1】 webportal ports *string*

〖参数说明〗<port number>m表示开启portal端口认证，<port number>-表示关闭portal端口认证。

〖命令模式〗配置模式

〖参考举例〗

- 开启 5、18 端口认证，关闭 1、20 端口认证
  switch(config)# portal ports 01-05m18m20-
  上述操作配置端口的认证控制状态。



在全局模式下键入show webportal ports查看端口的认证控制状态，即：

switch# show webportal ports

16.3 配置web/portal认证端口允许通过的主机数目

交换机中 web/portal 认证端口允许通过的主机数目缺省值是 256（最大值）。设定 web/portal 认证端口允许通过的主机数目，利用命令：

【命令1】webportal multiple-host-num *Number*

〖参数说明〗输入整数型数值，注意范围为1～256。
〖命令模式〗配置模式
〖参考举例〗

- 配置 web/portal 认证端口允许通过的主机数目为 10
  switch(config)# webportal multiple-host-num 10
  上述操作配置 web/portal 认证端口允许通过的主机数目。


在全局模式下键入show webportal multiple-host-num查看web/portal认证端口允许通过的主机数目，即：
switch# show webportal multiple-host-num

16.4 配置web/portal认证服务器ip地址

设定 web/portal 认证服务器 ip 地址，利用命令：

【命令1】webportal server-ip *ipaddr*

〖参数说明〗“ipaddr” 是指定的服务器的IP地址，类型是A.B.C.D。
〖命令模式〗配置模式
〖参考举例〗

- 配置 web/portal 认证服务器 ip 地址为 1.1.1.1
  switch(config)# webportal server-ip 1.1.1.1
  上述操作配置 web/portal 认证服务器 ip 地址。


在全局模式下键入show webportal server-ip查看web/portal认证服务器的ip地址，即： switch# show webportal server-ip

16.5 配置web/portal认证服务器udp端口号

交换机中 web/portal 认证服务器 udp 端口号缺省值是 20000。设定 web/portal 认证服务器 udp 端口号，利用命令：

【命令1】webportal server-udp *Number*

〖参数说明〗输入有效udp端口号。大于15000。

〖命令模式〗配置模式

〖参考举例〗

- 配置 web/portal 认证 udp 端口号为 16000
  switch(config)# webportal server-udp 16000
  上述操作配置 web/portal 认证服务器 udp 端口号。

☞ 在全局模式下键入show webportal server-udp查看web/portal认证服务器udp端口号，即： switch# show webportal server-ip

WEB CONFIG 16.5-1

认证

802.1x 认证 | Portal 认证 | Radius 服务器 | Radius 客户端

Portal 认证配置	
Portal认证服务	disable
Portal认证端口	20000
Portal服务器IP地址	0.0.0.0
每端口最大主机连接数	32

Portal认证端口选择

1 — 8	9 — 16	17 — 24
☑ ☑ ☑ ☑ ☑ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

第 17 章 配置 RADIUS

RADIUS （Remote Authentication Dial In User Service）远程用户拨号认证系统，是一个 client－server 模式的认证、授权、记账协议，它是通过 NAS 对试图连接到网络设备的用户进行认证的。NAS 对用户来说是一个接入服务器，对 RADIUS server 来说是一个客户机，称作 RADIUS client。NAS 通过与用户交互，得到用户的用户名、密码。然后，它将这些信息以及用户所连接的端口号、端口类型等信息封装成 RADIUS 报文后，传递给一个或更多的 RADIUS Server。然后，它根据从 RADIUS Server 收到的应答信息来决定是允许还是拒绝用户对网络设备的访问。用户认证成功后，NAS 可以定期地向 RADIUS Server 发送计费消息包，这些消息包可以反映出上网时间，输入输出流量等。RADIUS 使用 UDP 在 RADIUS client 和 server 之间传送 RADIUS 报文。

17.1 配置RADIUS CLIENT

◆ 打开或关闭 radius client 开关

交换机中 radius client 开关缺省状态是关闭的。设定 radius client 开启和关闭，利用命令：

【命令1】radiusclient service 〈*enable*/*disable*〉

〖参数说明〗enable表示开启radius client开关，disable表示关闭radius client 开关。

〖命令模式〗配置模式

〖参考举例〗

- 开启 radius client 开关
  switch(config)# radiusclient service enable
  上述操作打开 radius client 开关。

- 关闭 radius client 开关
  switch(config)# radiusclient service disable
  上述操作关闭radius client开关。

☞ 在全局模式下键入show radiusclient service查看是否设置成功，即：

switch# show radiusclient service

◆ 配置 radius clinet ip 地址

设定 radius client ip 地址,注意必须是已经配置过 vlan ip，否则配置不成功。利用命令：

【命令1】radiusclient ipaddress *ipaddr*

〖参数说明〗“ipaddr” 是IP地址，类型是A.B.C.D，输入有效ip地址，注意必须是已经配置过vlan ip。

〖命令模式〗配置模式

〖参考举例〗

- 配置 radius client 的 ip 地址为 1.1.1.1
  switch(config)# radiusclient ipaddress 1.1.1.1
  上述操作配置 radius client ip 地址。

☞ 在全局模式下键入show radiusclient ipaddress查看radius clinet ip地址，即：

switch# show radiusclient ipaddress

🎬WEB CONFIG 17.1-1

认证

802.1x 认证 | Portal 认证 | Radius 服务器 | Radius 客户端

Radius客户端配置	
客户端IP地址	0.0.0.0
实时记帐间隔	0
Raidus服务使能	disable

17.2 配置定时发送记账报文时间间隔

交换机中定时发送记账报文时间间隔缺省值为 0，也就是不启动定时发送记帐报文。设定定时发送记账报文时间间隔。利用命令：

【命令1】radiusclient accounting interval *Number*

〖参数说明〗输入整数型数值，单位为分钟，如果输入为0，表示关闭此功能；如果输入为2，也就时间间隔为2分钟。

〖命令模式〗配置模式

〖参考举例〗

- 配置定时发送记账报文时间间隔为 2 分钟
  switch(config)# radiusclient accounting interval 2
  上述操作配置定时发送记账报文时间间隔。

☞ 在全局模式下键入show radiusclient accounting interval查看定时发送记账报文时间间隔，即：

switch# show radiusclient accounting interval

17.3 配置radius服务器

◆ 设定 radius 主服务器 ip 地址

设定 radius 主服务器 ip 地址。利用命令：

【命令1】radiusserver master_ipaddress *ipaddr*

〖参数说明〗“ipaddr” 是指定服务器的IP地址，类型是A.B.C.D，输入有效ip地址，注意输入0.0.0.0，表示删除此IP地址。

〖命令模式〗配置模式

〖参考举例〗

- 配置 radius 主服务器的 ip 地址为 1.1.1.1
  switch(config)# radiusserver master_ipaddress 1.1.1.1
  上述操作配置 radius 主服务器 ip 地址。

☞ 在全局模式下键入show radiusserver master_ipaddress查看radius 主服务器ip地址，即：

switch# show radiusserver master_ipaddress

◆ 配置 radius 主服务器密钥

设定 radius 主服务器 密钥。利用命令：

【命令1】radiusserver master_key *String*

〖参数说明〗输入有效字符串，必须和radius服务器配置相对应。

〖命令模式〗配置模式

〖参考举例〗

- 配置 radius 主服务器的密钥为 test
  switch(config)# radiusserver master_key test
  上述操作配置 radius 主服务器的密钥。

☞ 在全局模式下键入show radiusserver master_key查看radius 主服务器 的密钥，即：

switch# show radiusserver master_key

◆ 配置 radius 主服务器认证、计费端口

交换机中 radius 主服务器认证端口缺省值为 1812，计费端口缺省为 1813。

【命令1】radiusserver master_port *<auth_num> <acct_num>*

〖参数说明〗*<auth_num>*认证端口号，*<acct_num>计费端口，*必须和radius服务器配置相对应。

〖命令模式〗配置模式
〖参考举例〗

- 配置 radius 主服务器的认证端口号为 1812
  switch(config)# radiusserver master_port 1812 1813
  上述操作配置 radius 主服务器的认证端口为 1812，计费端口为 1813。

☞ 在全局模式下键入show radiusserver master_port查看radius 主服务器 的认证端口和计费端口，即：

switch# show radiusserver master_port

♦ 配置 radius 从服务器 ip 地址

设定 radius 从服务器 ip 地址。利用命令：

【命令1】radiusserver slave_ipaddress *ipaddr*

〖参数说明〗“ipaddr” 是指定服务器的IP地址，类型是A.B.C.D，输入有效ip地址，注意输入0.0.0.0，表示删除此IP地址。
〖命令模式〗配置模式
〖参考举例〗

- 配置 radius 从服务器的 ip 地址为 1.1.1.1
  switch(config)# radiusserver slave_ipaddress 1.1.1.1
  上述操作配置 radius 从服务器 ip 地址。

☞ 在全局模式下键入show radiusserver slave_ipaddress查看radius 从服务器 ip地址，即：

switch# show radiusserver slave_ipaddress

♦ 配置 radius 从服务器密钥

设定 radius 从服务器 密钥。利用命令：

【命令1】radiusserver slave_key *String*

〖参数说明〗输入有效字符串，必须和radius服务器配置相对应。
〖命令模式〗配置模式
〖参考举例〗

- 配置 radius 从服务器的密钥为 test
  switch(config)# radiusserver slave_key test
  上述操作配置 radius 从服务器的密钥。

☞ 在全局模式下键入show radiusserver slave_key查看radius 从服务器 的密钥，即：

switch# show radiusserver slave_key

♦ 配置 radius 从服务器认证、计费端口

交换机中 radius 从服务器认证端口缺省值为 1812，计费端口缺省为 1813。

【命令1】radiusserver slave_port *<auth_num>* *<acct_num>*

〖参数说明〗*<auth_num>*认证端口号，*<acct_num>计费端口，*必须和radius服务器配置相对应。
〖命令模式〗配置模式
〖参考举例〗

- 配置 radius 从服务器的认证端口号为 1812，计费端口为 1813
  switch(config)# radiusserver slave_port 1812 1813
  上述操作配置 radius 从服务器的认证端口为 1812，计费端口为 1813。

☞ 在全局模式下键入show radiusserver slave_port查看radius 主服务器 的认证端口和计费端口，即：

switch# show radiusserver slave_port

WEB CONFIG 17.3-1

认证

802.1x 认证 | Portal 认证 | Radius 服务器 | Radius 客户端

Radius主服务器配置	
主服务器认证密钥	
主服务器IP地址	0.0.0.0
主服务器认证端口	1812
主服务器计费端口	1813

Radius从服务器配置	
从服务器认证密钥	
从服务器IP地址	0.0.0.0
从服务区认证端口	0
从服务器计费端口	0

第 18 章 配置 DHCP Relay

DHCP Relay可以在跨网段的情况下实现动态地址分配，即DHCP服务器与客户机可以不在相同的子网内，无须在每个子网内都放置DHCP服务器，各子网分支可以统一使用一个DHCP服务器来获取地址，便于大型网络的规划管理。

18.1 打开或关闭dhcp relay开关

交换机中 dhcp relay 缺省状态是关闭的。设定 dhcp relay 开启和关闭，利用命令：

【命令1】 dhcpr service <*enable*/*disable*>

〖参数说明〗enable表示开启dhcp relay开关，disable表示关闭dhcp relay开关。
〖命令模式〗配置模式
〖参考举例〗

- 开启 dhcp relay 开关
  switch(config)# dhcpr service enable
  上述操作打开 dhcp relay 开关。

- 关闭 dhcp relay 开关
  switch(config)# dhcpr service disable
  上述操作关闭dhcp relay开关。

☞ 在全局模式下键入show dhcpr service查看是否设置成功，即：

switch# show dhcpr service

WEB CONFIG 18.1-1



18.2 配置dhcp server

◆ 配置 dhcp server ip 地址

设定 dhcp server ip 地址，利用命令：

【命令1】dhcpr targetip add *Number ipaddr*

〖参数说明〗Number为dhcp server ip的索引，ipaddr为ip地址，类型为< A.B.C.D >。
〖命令模式〗配置模式
〖参考举例〗

● 配置索引为 1 的 dhcp server 的 ip 地址为 1.1.1.1
switch(config)# dhcpr targetip add 1 1.1.1.1
上述操作配置 dhcp server ip 地址。

☞ 在全局模式下键入show dhcpr targetip查看所有配置过的dhcp server ip地址，即：

```
switch# show dhcpr targetip
```

♦ 删除 dhcp server ip 地址

删除 dhcp server ip 地址，利用命令：

【命令1】dhcpr targetip del *Number*

〖参数说明〗Number为dhcp server ip的索引。
〖命令模式〗配置模式
〖参考举例〗

● 删除索引为 1 的 dhcp server 的 ip 地址
switch(config)# dhcpr targetip del 1
上述操作删除 dhcp server ip 地址。

☞ 在全局模式下键入show dhcpr targetip查看所有配置过的dhcp server ip地址，即：

```
switch# show dhcpr targetip
```

WEB CONFIG 18.2-1

DHCP中继服务

DHCP 服务设置 | DHCP 侦听 | DHCP 服务器地址

DHCP 服务器IP地址	
序号	
IP地址	0.0.0.0

序号	IP地址
0	0.0.0.0
1	0.0.0.0
2	0.0.0.0
3	0.0.0.0
4	0.0.0.0

18.3 配置dhcp 侦听

- 设定侦听 dhcp 消息的虚拟接口

【命令1】dhcpr listen add *Number ifname*

〖参数说明〗Number为dhcp侦听vlan的索引， ifname为已经配置过虚拟接口的名字，如vint0。

〖命令模式〗配置模式

〖参考举例〗

- 配置 vint1 侦听 dhcp 消息，索引为 1

  switch(config)# dhcpr listen add 1 vint1

☞ 在全局模式下键入show dhcpr listen查看所有配置过的侦听dhcp消息的虚拟接口，即：

switch# show dhcpr listen

- 取消虚拟接口侦听 dhcp 消息

【命令1】dhcpr listen del *Number*

〖参数说明〗 Number为dhcp侦听的索引。

〖命令模式〗配置模式

〖参考举例〗

- 取消索引为 1 的虚拟接口侦听 dhcp 消息

```
switch(config)# dhcpr listen del 1
```

☞ 在全局模式下键入show dhcpr listen查看所有配置过的侦听dhcp消息的虚拟接口，即：

```
switch# show dhcpr listen
```

WEB CONFIG 18.3-1

DHCP中继服务

DHCP 服务设置 | DHCP 侦听 | DHCP 服务器地址

DHCP 中继侦听	
序号	
虚拟接口	none

序号	虚拟接口
0	
1	
2	

第 19 章 配置 DHCP Server

本章主要介绍系统内嵌的 DHCP 服务器配置，使用内嵌的 DHCP 服务器，用户无须另外配备专门的 DHCP 服务器，降低了网络建设和维护成本，比较适合于中小型网络应用。

19.1 打开或关闭dhcp server开关

交换机中 dhcp server 缺省状态是关闭的。设定 dhcp server 开启和关闭，利用命令：

【命令1】 dhcps service *<enable/disable>*

〖参数说明〗enable表示开启dhcp server开关，disable表示关闭dhcp server开关。

〖命令模式〗配置模式

〖参考举例〗

- 开启 dhcp server 开关

  switch(config)# dhcps service enable

  上述操作打开 dhcp server 开关。

- 关闭 dhcp server 开关

  switch(config)# dhcps service disable

  上述操作关闭dhcp server开关。

☞ 在全局模式下键入show dhcps service查看是否设置成功，即：

switch# show dhcps service

注意：要使能dhcp server，必须先配置dhcps listen add *<Number>* *<Vlanname>*!

19.2 配置侦听dhcp消息虚拟接口

【命令1】 dhcps listen add *< Number >* *< Vlanname >*

〖参数说明〗< Number >为dhcp侦听vlan的索引，< Vlanname >为已经存在的虚拟接口

〖命令模式〗配置模式

〖参考举例〗

- 配置 vint1 侦听 dhcp 消息，索引为 1

  switch(config)# dhcps listen add 1 vint1

☞ 在全局模式下键入show dhcps listen查看所有配置过的侦听dhcp消息的虚拟接口，即：

switch# show dhcps listen

注意：如果dhcp server已经使能，再添加listen interface，必须重新使能dhcp server，这样新添加的interface才可以起作用！

更改listen配置的内容的时候，同时dhcp relay的listen配置也会更改！

19.3 取消虚拟接口侦听dhcp消息

【命令1】dhcps listen del ＜ *Number* ＞

〖参数说明〗＜ Number ＞为dhcp侦听的索引。
〖命令模式〗配置模式
〖参考举例〗

- 取消索引为 1 的虚拟接口侦听 dhcp 消息
  switch(config)# dhcpr listen del 1

☞ 在全局模式下键入show dhcps listen查看所有配置过的侦听dhcp消息的虚拟接口，即：

```
switch# show dhcpr listen
```

19.4 设置默认的DNS服务器地址

设置默认的 DNS 服务器地址，利用命令：

【命令1】dhcps dns ＜ *A.B.C.D* ＞
〖参数说明〗输入有效ip地址。
〖命令模式〗配置模式
〖参考举例〗

- 配置默认的 DNS 服务器地址为 202.96.128.68
  switch(config)# dhcps dns 202.96.128.68
  上述操作配置默认的 DNS 服务器地址。

☞ 在全局模式下键入show dhcps dns查看是否设置成功，即：

```
switch# show dhcps dns
```

19.5 设置默认的ip地址租期

系统默认时间为 691200（八天），设置默认的 ip 地址租期，利用命令：

【命令1】dhcps leasetime ＜ *time* ＞
〖参数说明〗输入有效时间，单位为秒。0视为无效值。
〖命令模式〗配置模式
〖参考举例〗

- 配置默认的 ip 地址租期为 86400 秒（一天）

  switch(config)# dhcps leasetime 86400

  上述操作配置默认的 ip 地址租期。

在全局模式下键入show dhcps leasetime查看是否设置成功，即：

switch# show dhcps leasetime

19.6 添加dhcp server地址池

添加 dhcp server 地址池，利用命令：

【命令1】dhcps addresspool add *Name StartIp EndIP Gateway Netmask* [DNS1 〈*dns1*〉 DNS2 〈*dns2*〉 leasetim 〈*leasetim* 〉 params *string*]

〖参数说明〗"*Name*"是地址池的名字，"*StartIp*"起始IP地址，类型为A.B.C.D，"*EndIp*"结束IP地址，类型为A.B.C.D，"*Netmask*"子网掩码，类型为A.B.C.D，〈*dns1*〉是主DNS的IP 地址，类型为A.B.C.D；〈*dns2*〉是从DNS的IP 地址，类型为A.B.C.D；〈*leasetim* 〉租期，单位为秒。

〖命令模式〗配置模式

〖参考举例〗

- 添加 dhcp server 地址池

  switch(config)# dhcps addresspool add vlan1 1.1.1.1 1.1.1.100 1.1.1.200 255.255.255.0

  上述操作添加 dhcp server 地址池名字为 vlan1，地址范围 1.1.1.1-1.1.1.100，网关为 1.1.1.200，子网掩码为 255.255.255.0

注意：DNS1，DNS2，Leasetime 可以为空，如果为空的，就用默认的 DNS 和 Leasetime 配置！ Params 一般都为空，是为了用于配置 dhcp server 地址池其他扩充属性！

在全局模式下键入show dhcps addresspool查看所有配置过的dhcp server的地址池，即：

switch# show dhcps addresspool

19.7 删除dhcp server地址池

删除 dhcp server 地址池，利用命令：

【命令1】dhcps addresspool del 〈 *name* 〉

〖参数说明〗输入已经配置过的地址池的名字

〖命令模式〗配置模式

〖参考举例〗

- 删除名字为 vlan1 的地址池

  switch(config)# dhcps addresspool del vlan1

  上述操作删除 dhcp server 地址池名字为 vlan1



在全局模式下键入show dhcps addresspool查看所有配置过的dhcp server的地址池，即：

```
switch# show dhcps addresspool
```

第 20 章 配置 SNMP

本章首先简述 SNMP 协议的原理和基本参数的介绍，然后介绍交换机的 SNMP 配置方法。

20.1 SNMP协议简介

简单网络管理协议（SNMP：Simple Network Management Protocol）是由互联网工程任务组（IETF：Internet Engineering Task Force ）定义的一套网络管理协议。利用 SNMP，一个管理工作站可以远程管理所有支持这种协议的网络设备，包括监视网络状态、修改网络设备配置、接收网络事件警告等。

SNMP 采用了 Client/Server 模型的特殊形式：代理/管理站模型。对网络的管理与维护是通过管理工作站与 SNMP 代理间的交互工作完成的。每个 SNMP 从代理负责回答 SNMP 管理工作站（主代理）关于 MIB 定义信息的各种查询。

下面介绍 SNMP 协议的一些基本参数

- **版本识别符（version identifier)**：确保 SNMP 代理使用相同的协议，每个 SNMP 代理都直接抛弃与自己协议版本不同的数据报。

- **团体名（Community Name)**：用于 SNMP 代理对 SNMP 管理站进行认证；如果网络配置成要求验证时，SNMP 代理将对团体名和管理站的 IP 地址进行认证，如果失败，SNMP 代理将向管理站发送一个认证失败的 Trap 消息；

- **协议数据单元（PDU)**：其中 PDU 指明了 SNMP 的消息类型及其相关参数。

- **管理信息库 MIB**：IETF 规定的管理信息库 MIB（定义了可访问的网络设备及其属性，用对象识别符（OID：Object Identifier）唯一指定。MIB 是一个树形结构，SNMP 协议消息通过遍历 MIB 树形目录中的节点来访问网络中的设备。

20.2 配置SNMP

配置 snmp 团体

【命令1】 snmp community set *number string <read-only/read-write>*

〖参数说明〗“string”, 团体名称，为字符串；
“number” 团体号，范围是1-8；
< *read-only / read-write*> 访问权限，即属性值，*read-only*表示只读，*read-write*表示可读写。

〖命令模式〗配置模式

〖参考举例〗 switch(config)# snmp community set 2 public read-write
上述命令设置 2 号团体的名字是 public,其属性值是读写。

☞ 在全局模式下键入show snmp community查看配置是否成功，即：

switch# show snmp community

删除 snmp 团体

【命令2】snmp community delete *number*
〖参数说明〗 “number” 团体号，范围是1-8;
〖命令模式〗 配置模式
〖参考举例〗 switch(config)# snmp community delete 2
上述命令删除 2 号团体。

☞ 在全局模式下键入show snmp community查看配置是否成功，即:
switch# show snmp community

WEB CONFIG 20.2-1



设置陷阱发送的服务器地址

【命令3】snmp traps host *entrynum* hostaddr *hostaddr* port *port*
〖参数说明〗 “entrynum” 表示该配置项的序号，范围是1-3;
“hostaddr”管理服务器的IP地址，类型是A.B.C.D
“port” 服务器接收trap信息的端口，缺省值是162。
〖命令模式〗 配置模式
〖参考举例〗switch(config)# snmp traps host 1 hostaddr 2.2.2.2 port 162
上述命令设置 snmp 陷阱发送的目的服务器的地址（2.2.2.2）和端口号(162)。

☞ 在全局模式下键入show snmp traps查看配置是否成功，即:
switch# show snmp traps

WEB CONFIG 20.2-2

网管协议(SNMP)

Community 设置 | Trap 设置

SNMP 目标IP地址				
序号	传送IP地址	超时设置	重试次数	状态
1	0.0.0.0	1500	3	notReady
1	0.0.0.0	1500	3	notReady
2	0.0.0.0	1500	3	notReady
3	0.0.0.0	1500	3	notReady

SNMP 目标参数					
序号	报文处理模块	安全模型	安全名	安全级别	状态
1	0	1	public	noAuthNoPriv	active
1	0	1	public	noAuthNoPriv	active
2	1	2	public	noAuthNoPriv	active
3	3	3	initialnone	noAuthNoPriv	active

设置陷阱参数

【命令4】 snmp traps parameters *entrynum* mpmodel < *v1/ v2c/ v3*> securemodel < *v1/ v2c/ usm*> securename *name* securelevel *<noAuthNoPriv/AuthNoPriv/AuthPriv>*

〖参数说明〗 “entrynum” 表示该配置项的序号，范围是1-3；

其他参数见下面附加说明。

〖命令模式〗 配置模式

〖参考举例〗 switch(config)# snmp traps parameters 1 mpmodel v2c securemodel v2c securename snmptest securelevel AuthNoPriv

上述命令设置 snmp 报文处理模式是 snmpv2c 模式，安全模式是 snmpv2 安全模式，安全名字 snmptest,安全级别是认证不加密模式。

 在全局模式下键入show snmp traps查看配置是否成功，即：

switch# show snmp traps

陷阱参数附加说明

MP Model：Message Processing Model的简写，也即报文处理模块。在RFC2571描述的SNMPv3管理框架中，把以前版本所叫的管理站和代理等统一叫做SNMP实体(SNMP entity)。实体结构中的的SNMP引擎包括报文处理子系统和安全子系统等，Mp Model即输入报文处理子系统。每一个报文处理模块定义了一种特殊的SNMP报文格式,它的功能是按照预定的格式准备要发送的报文，或者从接收的报文中提取数据。这种体系结构允许扩充其他的报文处理模块，扩充的处理模块可以是企业专用的，也可以是以后的标准添加的。每一个报文处理模块都定义

了一种特殊的SNMP报文格式，以便能够按照这种格式生成报文,或从报文中提取数据。在交换机中，MP Model参数设为0代表采用SNMPv1报文处理模型，为1代表SNMPv2c报文处理模型，为3代表SNMPv3报文处理模型。

Security Model和Security Name：即安全模型和安全名，属于SNMP引擎中的安全子系统。当一个SNMP实体处理检索(get、get-next等)或修改(set)请求都要检查是否允许访问指定的管理对象，以及是否允许执行请求的操作，当SNMP实体产生通知报文时也要用到访问控制机制，以决定把消息发送给谁。在SNMPv3中，采用基于视图的访问控制模型(VACM)。安全模型和安全名以及下面所讲的安全级别(Security Level)都属于VACM用到的概念。在安全子系统中，有一个组(Group)的概念，由二源组<securityModel, securityName>的集合构成。属于同一组的所有安全名在指定的安全模型下的访问权限相同。在交换机中，Security Model为1代表SNMPv1方式，为2代表SNMPv2c的安全模型，为3代表USM，即基于用户的安全模型（User-Based Security Model）。
Security Level：在同一组中成员可以有不同的安全级别，即noAuthNoPriv（无认证不保密）、authNoPriv(有认证不保密)和authPriv(有认证要保密)。任何一个访问请求都有相应的安全级别。

第 21 章 配置 ARP

本章介绍ARP表的静态配置。

设置静态ARP表

【命令1】arp add *ipaddr macaddr*

〖参数说明〗 “ipaddr” 表示所添加的ARP表项的IP地址，类型为A.B.C.D,注意IP地址应该是系统所包含的网段地址；

“macaddr” 表示所添加的ARP表项的MAC地址，类型为xx:xx:xx:xx:xx:xx

〖命令模式〗 配置模式

〖参考举例〗 switch(config)# *arp add 192.168.1.234 00:02:11:20:03:11*

上述命令配置 192.168.1.23 的映射的 mac 地址是 00:02:11:20:03:11。

☞ 在全局模式下键入show arp查看配置是否成功，即：

switch# show arp

注意：

IP地址应该是系统所包含的网段地址。

删除 ARP 表项

【命令2】arp delete *ipaddr*

〖参数说明〗 “ipaddr” 表示所添加的ARP表项的IP地址，类型为A.B.C.D,注意IP地址应该是系统所包含的网段地址；

〖命令模式〗 配置模式

〖参考举例〗 switch(config)# *arp delete 192.168.1.234*

上述命令将删除 192.168.1.234 所对应的 mac 地址映射。

清空动态 ARP 表项

【命令2】arp flush

〖参数说明〗 无参数

〖命令模式〗 配置模式

〖参考举例〗 switch(config)# arp flush

上述命令将清空所有动态学习到的 ARP 表项，静态的并不被删除。

注意：

静态的ARP表项并不被删除。

附录　常见故障诊断

故障现象	可能的故障原因	解决方法
加电时所有指示灯均不亮	电源连接错误或供电不正常	检查电源线和插座
LINK 指示灯不亮	1．网线损坏或连接不牢。 2．网线类型错误或网线过长，超出允许范围。	更换网线。
LINK 指示灯闪烁	1．网线接线不标准。 2．网线过长，超出允许范围。	更换或重做网线。
网络能通，但传输速度变慢，有丢包现象	交换机与网络终端以太网口工作模式不匹配。	设置以太网口工作模式使其匹配或将其设为自适应工作模式。
在某一口可通，将网线换到其他口时则不通	将网线换到其他网口时，如果此端口所连接的设备没有发送数据，交换机将学不到新地址，因此此端口会暂时不通。	150 秒后交换机的地址会自动更新，此现象会自动消失。或者从此网口发送数据也会使交换机立即更新其地址表。
所有 ACT 指示灯闪烁，网络速率变慢	广播风暴	1、检查网络连接是否成环路，合理配置网络。 2、检查是否有站点发送大量的广播包。
正常工作一段时间后停止工作	1．电源不正常。 2．过热。	1.检查电源是否有接触不良，电压过低或过高。 2．检查周围环境，通风孔是否畅通，交换机风扇是否工作正常。
不能通过 Telnet 访问系统	1．网络连接不正确 2．IP 地址未配置	1．检查网络连接。 2．通过串口访问系统，正确配置 IP 地址。